Winter 1-2021

SIGURIA KIBERNETIKE GJATË PUNËS NGA DISTANCA

Agon Daci
University for Business and Technology - UBT

Programi për Shkenca Kompjuterike dhe Inxhinierise

SIGURIA KIBERNETIKE GJATË PUNËS NGA DISTANCA

Shkalla Bachelor

Agon Daci

Janar / 2021
Prishtinë

Programi për Shkenca Kompjuterike dhe Inxhinierise

Punim Diplome
Viti akademik 2015 – 2018

Agon Daci

SIGURIA KIBERNETIKE GJATË PUNËS NGA DISTANCA

Mentori: Dr. Blerton Abazi

Janar / 2021

Ky punim është përpiluar dhe dorëzuar në përmbushjen e kërkesave të pjesshme për Shkallën Bachelor

ABSTRAKT

Në çdo pjesë të përditshmërisë dhe jetës tonë kemi vendosur përdorimin e teknologjisë së informacionit dhe sistemet e informacionit në përgjithësi. Jeta e jonë është e plotësuar me Internetin e gjërave (IoT), ku shtëpitë tona tani janë shtëpi të mençura.

Mundësitë për të thjeshtësuar dhe lehtësuar punën tonë janë shumë të mëdha dhe tani në këtë realitet që jetojmë, kemi mundësi të përfundojmë detyrat tona edhe pa prezencën fizike, nga distanca.

Puna nga distanca ka shumë përparësi sa i përket anës ekonomike sikurse të punonjësit ashtu edhe të punëdhënësit që mund të kursejmë në hapësirë (qira, objekt, udhëtim), më tepër liri të veprimit duke rritur produktivitetin larg nga shpërqendrimet e zyrës, bashkëpunimin në lokacione të ndryshme. Si dhe, sigurimin e shëndetit në rast pandemie sikurse tani që kemi pandeminë COVID19.

Gjithë kjo përparësi që na ofron teknologjia për lehtësimin e përditshmërisë tonë përmes internetit na ekspozon në botën e jashtme dhe na cenon privatësinë dhe sigurinë tonë. Pa marr parasysh që jemi në shtëpitë tona të rrethuar me mure të forta dhe kemi porta me kyçe të sigurisë së lartë jemi përsëri të rrezikuar nga vetëm një port komunikimi aq i vogël sa është porti i internetit, mirëpo që na ekspozon në gjithë globin. Prandaj siguria ndaj sulmeve kibernetike çdo ditë e më shumë është duke u bërë më sfiduese për t'u menaxhuar.

Duke qenë kaq me rëndësi ne do të trajtojmë këtë temë me shumë kujdes duke shpjeguar në detaje dhe analizuar edhe raste studimi për të marr shembull dhe nxjerrë konkluzione mbi sigurinë kibernetike gjatë punës nga distanca.

Ideja për këtë temë vjen si rrjedhojë e aktualitetit që kemi në shumicën e bizneseve, institucioneve dhe veprimtarive në të cilat është duke u zbatuar puna nga distanca. Si pasojë e përballjes me pandeminë COVID19, duke ngritur nevojën më të theksuar për siguri kibernetike përgjatë punës nga distanca.

FALËNDERIM

Kjo temë nuk do të ishte shkruar pa mbështetjen e këtyre personave që u jam shumë mirënjohës:

Së pari do të doja t'i shprehja mirënjohjet e mia më të sinqerta mentorit tim Prof. Blerton Abazi, i cili më dha kurajon dhe lirinë e nevojshme të punojë këtë temë.

Gjithashtu, mirënjohje i shpreh gjithë departamentit të Shkencave Kompjuterike për periudhën e studimeve të mia Bachelor këtu në Universitetin për Biznes dhe Teknologji – UBT në Prishtinë.

Kam qenë shumë me fat që kam pasur përkrahjen e shumë miqve të mirë.

I detyrohem shumë familjes sime, veçanërisht prindërve të mi, të cilët më kanë dhënë kurajo dhe më kanë ndihmuar në çdo hap të jetës sime personale dhe akademike dhe me mezi kanë pritur të shohin këtë arritje timen. Faleminderit shumë për dashurinë dhe përkrahjen e dhënë. Kjo temë ju dedikohet juve.

PËRMBAJTJA

LISTA E FIGURAVE

LISTA E TABELAVE

LISTA E SHKURTESAVE

TI - Teknologji Informative

ARPANET - Advanced Research Projects Agency Network

MIT - Massachusetts Institute of Technology

RSA - Rivest Shamir Adleman

SSL - Secure Socket Layer

HTTPS - Hyper Text Transfer Protocol Secure

DDoS - Distributed Denial of Service

SHBA - Shtetet e Bashkuara të Amerikës

BE - Bashkimi Evropian

GDPR - General Data Protection Regulation

AI - Artificial Intelligence

WI-FI - Wireless Fidelity

USB - Universal Serial Bus

WPA2 - Wi-Fi Protected Access 2

SFTP - Secure File Transfer Protocol

USA - United States of America

IoT - Internet of Things

IBM - International Business Machines

CEO - Chief Executive Officer

AT&T - American Telephone and Telegraph

GTM - GoToMeeting

OBSH - Organizata Botërore e Shëndetësisë

H2H - Human to Human

PPE - Personal Protective Equipment

NCSC - National Cyber Security Center

DHS - Department of Homeland Security

CISA - Cybersecurity and Infrastructure Security Agency

HMRC - Her Majesty's Revenue and Customs

NHS - National Health Service

URL - Uniform Resource Locator

SS7 - Sistemin e Sinjalizimit 7

2FA - Two Factor Authentication

SMSC - Short Message Service Center

LLP - Limited Liability Partnership

FBI - Federal Bureau of Investigation

ET - Eastern Time

WIRED - Workforce Innovation in Regional Economic Development

VPN - Virtual Private Network

SIM - Subscriber Identity Module

DOJ - Department of Justice

NYSDFS - New York State Department Financial Services

SIEM - Secure Incident Event Management

SHIELD - Stop Hacks and Improve Electronic Data Security

VAPT - Valued Assessment Penetration Tests

BEC - Business Email Compromise

DMARC - Domain-based Message Authentication, Reporting & Conformance

SPF - Sender Policy Framework

DKIM - DomainKeys Identified Mail

1 HYRJE

Interneti ka ndryshuar botën dhe jetën tonë, duke na ofruar shumë mundësi, gjithnjë e më shumë njerëzit po marrin përfitimet e punës në internet. Kjo ka çuar në rritjen e krijimit të vendeve të punës në të gjithë globin. Për më tepër, disa organizata që janë bazuar vetëm në internet lejojnë që punonjësit e tyre të punojnë edhe nga shtëpia. Gjithashtu, disa punonjës, përveç nëse kanë takime, përndryshe nuk do të paraqiten kurrë në zyrën e tyre. Mundësitë që ofron interneti nga postat elektronike, aplikacionet e mesazheve si Slack, Google Meet, Zoom, Microsoft Teams dhe madje edhe Skype, duke punuar nga shtëpia, ose dikush edhe në pjesë të ndryshme të botës.

Puna nga distanca që shpesh në botën e TI-së e hasim edhe me termet "Telekomunikimi" apo "Telework" deri vonë është menduar si puna e së ardhmes, në ditët e sotme ka arritur të bëhet një realitet i përditshmërisë tonë, sidomos pas fillimit të përballjes me pandeminë COVID19.

Puna nga distanca është punë e realizuar zakonisht nga shtëpia, apo punë e realizuar nga kudo, mirëpo jashtë objektit zyrtar të punës, përmes kompjuterit personal, celularit dhe pajisjeve të tjera komunikuese.

Duket se gjithçka tani mbështetet te kompjuterët dhe interneti, komunikimi (e-mail, telefona të mençur, tableta), argëtim (lojëra, video, media sociale, aplikacione), transport (sisteme navigimi, automjete të mençura), blerje (pazar në internet, karta krediti), mjekësi (pajisje mjekësore, regjistra mjekësorë, receta mjekësore). Lista vazhdon duke u rritur me shfrytëzimin e mundësisë së punës në distancë apo nga shtëpia, sidomos në vitin e fundit pas goditjes nga pandemia COVID19. Çdo ditë e përditshmërisë tonë është duke u mbështetur në teknologji. Pothuajse çdo informacion personal e ruajmë në kompjuterët tanë, telefona të mençur, tabletë ose në ndonjë sistem tjetër që e shfrytëzojmë.

Mirëpo, cilat janë saktësisht përparësitë dhe mangësitë e punës nga distanca?

Njëra ndër përparësitë është udhëtimi. Kërkimet kanë treguar se harxhohet shumë kohë kur punonjësit duhet të lëvizin për të punuar, të jesh në gjendje të punosh në internet do të thotë që je në gjendje të shmangësh nxitimin e trafikut nga dhe drejt punës.

Një tjetër përparësi është koha cilësore familjare. Puna në internet mund t'ju lejojë të punoni nga shtëpia duke ju dhënë fleksibilitetin shumë të nevojshëm për të kaluar kohën me familjen tuaj. Kursimi në kosto është një nga avantazhet e punës në internet. Gjithashtu, puna në internet ju bën më fleksibël dhe do të thotë që të jeni në gjendje të punoni nga kudo.

Ndërsa mangësitë apo disavantazhet e punës nga distanca janë këto:

Puna nga shtëpia mund të ju bëj më përtacë. Mungesa e vetë-disiplinës mund ta bëjë njeriun të bëhet më pak produktiv dhe të jetë më i shpërqendruar. Punët e shtëpisë, mund të ju marrin më shumë kohë kur jeni duke punuar nga shtëpia, duke marr kohën tuaj të punës dhe duke ju lënë me detyra të papërfunduara që vazhdojnë të grumbullohen çdo ditë.

Mundësitë e humbura të rrjetit. Duke u bërë më pak social dhe më pak të interesuar për të shkuar në ngjarje të rrjetit shoqëror. Dhe gjithashtu, duke u bërë më të varur nga interneti. Në rast të ndërprerjes së energjisë, apo internetit, do të detyroheni të humbni disa orë kohë pune duke ndikuar në afatet tuaja dhe duke mos qenë në gjendje të kryeni asnjë punë në mungesë të internetit.

Në mesin e të gjitha përparësive që kemi nga përdorimi i internetit për punën nga distanca ne jemi gjithashtu te ekspozuar edhe ndaj një mangësie që mund të na vjen me përdorimin e internetit, ajo është një nga gjërat esenciale për jetën e një njeriu – siguria, siguria kibernetike.

Krahas zhvillimit të hovshëm të teknologjisë së informacionit dhe përfshirjes së saj në çdo fushë, duke ndikuar në ndryshimin, avancimin dhe zhvillimin e jetës sonë të përditshme, është bërë shumë e nevojshme edhe siguria kibernetike.

Siguria kibernetike është arti i mbrojtjes së rrjeteve, pajisjeve dhe të dhënave nga hyrja e paautorizuar ose përdorimi kriminal dhe praktika e sigurimit të konfidencialitetit, integritetit dhe disponueshmërisë së informacionit. [1]

Zbatimi i masave efektive të sigurisë kibernetike është mjaft sfidues sot, sepse ka më shumë pajisje sesa njerëz dhe sulmuesit po bëhen më inovativë. Prandaj, zhvillohen praktikat e mbrojtjes së sistemeve, rrjeteve dhe programeve nga sulmet dixhitale, të cilat kanë për qëllim qasjen, ndryshimin ose shkatërrimin e informacioneve të ndjeshme, si përfitime financiare nga përdoruesit ose ndërprerjen e proceseve normale dhe dëmtimin e biznesit.

2 SHQYRTIMI I LITERATURËS (HISTORIKU)

Gjatë hulumtimit ne kemi rishikuar shumë raste studimi dhe praktika për sigurinë kibernetike dhe organizimin e punës nga distanca, por gjithashtu kemi konsultuar edhe fillesat e para dhe historinë e këtyre dy çështjeve të cilat më pas edhe i trajtojmë gjatë këtij punimi.

2.1. Siguria kibernetike, zhvillimi i historisë së saj ndër vite

Sot, siguria kibernetike është kryesore në mendjen e të gjithëve. Por kur versioni i parë i internetit u shfaq një gjysmë shekulli më parë, siguria as nuk ishte në skicë. Fokusi teknik ishte mënyra se si të funksionojë kjo skemë e re e rrjeteve e bazuar në paketa. Siguria nuk i shkonte në mendje grupit të ngushtë të akademikëve hulumtues që i besonin njëri-tjetrit, ishte e pamundur në atë kohë që dikush tjetër të hynte në rrjetin e ri. [2]

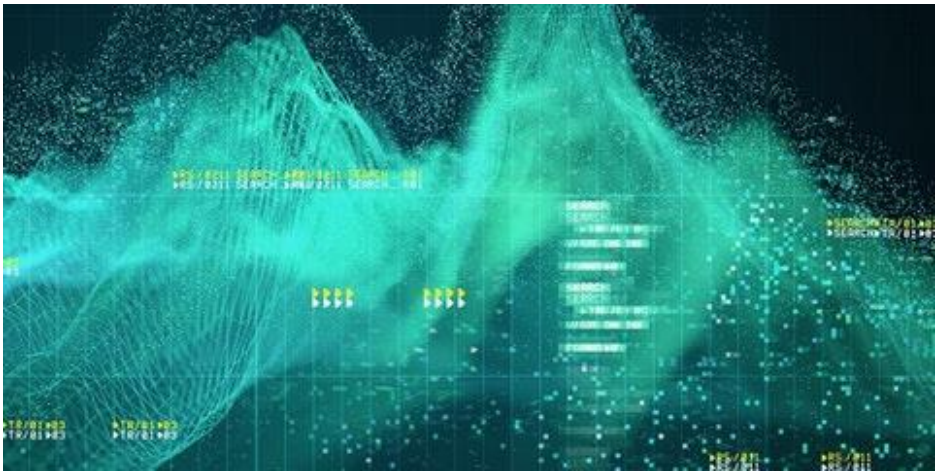

Figure 1. Zhvillimi i TI-së pa sigurinë kibernetike në mendje[1]

Në fillimin e viteve 1990, nuk kishte ligje për krime kompjuterike dhe shumica e "hakerave" ishin thjesht njerëz kuriozë - jo si hakerat dashakeqë të sotëm që janë për të shkatërruar gjëra. [3]

[1] Burimi: https://www.futureoftech.org/cybersecurity/2-history-of-cybersecurity/

Me përhapjen e sotme të përdorimit të internetit dhe dobisë së tij në retrospektivë, kemi edhe një rritje moderne të sulmeve kibernetike dhe është e lehtë të shohësh se si injorimi i sigurisë ishte një e metë madhe.

Disa ndryshime kanë ndodhur kaq shpejt sa është bërë e vështirë të thuash ndryshimin midis trendëve kalimtar, zhvillimit të sjelljes dhe diçkaje që tashmë është bërë një normë e pranueshme shoqërore. Për t'i bërë gjërat më të thjeshta, do t'i referohem realitetit ballë për ballë si "jeta reale" ose "bota reale" për ta veçuar atë nga hapësira kibernetike, megjithëse jemi plotësisht të vetëdijshëm se çfarë mund të ndodhë atje mund të jetë aq e vërtetë sa çdo gjë reale. Normat e reja të krijuara në internet mund të migrojnë në jetën reale. Pra, ajo që ndodh në botën virtuale ndikon në botën reale dhe anasjelltas.

Interneti është i kudondodhur, gjithmonë duke dhënë përmbajtje të pasur, stimuluese - gjithë ditën, tërë natën, gjithnjë aktiv. Midis viteve 2000 dhe 2015, numri i njerëzve me qasje në internet u rrit pothuajse shtatë herë - nga 6.5% në 43 % të popullatës globale. Në Samitin e Davosit në janar 2016, u njoftua se më shumë se 3.2 miliardë njerëz janë tani në internet. Në më pak se dhjetë vjet, numri i kyçjeve në celular është rritur nga pak më shumë se 2 miliardë në 2005 në më shumë se 7 miliardë në 2015. Numri i orëve që njerëzit kalojnë në celular po përshkallëzohet me shpejtësi çdo vit, duke kërcyer mesatarisht 65% në një periudhë dy vjeçare. I njëjti studim zbuloi se përdoruesit e telefonit celular kontrolluan pajisjet e tyre më shumë se pesëmbëdhjetë herë në javë dhe ka disa aplikacione që do ta llogarisin atë për ju, nëse keni nevojë për një ndihmë të vogël për të menaxhuar zakonin tuaj. [4]

Numri i minutave në ditë që ju kaloni duke kontrolluar telefonin tuaj dhe duke lëvizur nëpër postimet e mediave sociale nuk është i parëndësishëm. Për një hulumtues, i cili studion sjelljen njerëzore në minutë pas minute - në gjurmë dixhitale - këto minuta tregojnë se si po jeton një person - çfarë bënë dhe çfarë nuk bënë. Ky quhet modeli i analizës së jetës, ose mënyra se si njerëzit jetojnë në internet. Në shtëpi, këto minuta nuk janë shpenzuar duke bërë gjëra të tjera - duke lexuar një libër për një fëmijë, duke luajtur me një vogëlush në dysheme, duke biseduar me familjen tuaj në tryezën e darkës, duke biseduar me partnerin tuaj para gjumit. Kur jeni duke kontrolluar telefonin tuaj ose po kaloni kohë duke shfletuar faqet e internetit, ju jeni në të vërtetë në një mjedis tjetër. Ju keni shkuar diku tjetër. Ju nuk jeni i pranishëm në terma të botës reale. [4]

Nëse shohim prapa në ngjarjet e sigurisë, historia relativisht e shkurtër e sigurisë kibernetike vë në pah momente të rëndësishme dhe mësime se ku po shkon industria.

Në vazhdim kemi disa nga ngjarjet kryesore që ndihmojnë të kuptohet se si kemi arritur në pikën e sotme të sigurisë kibernetike. Duke filluar në vitet 1970, me zbulimin e parë të një virusi kompjuterik.

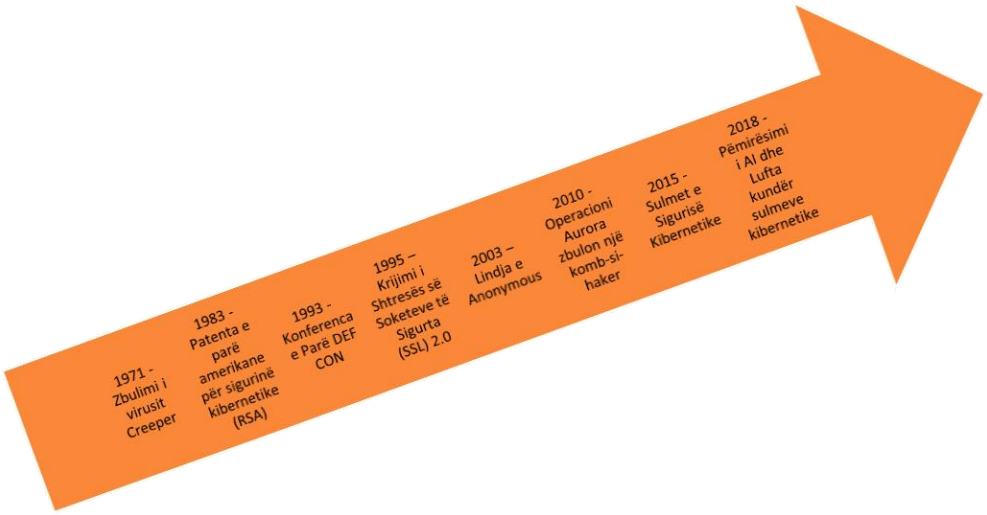

Figure 2. Ngjarjet kryesore të sigurisë kibernetike ndër vite

2.1.1. 16 mars 1971 - Zbulimi i virusit Creeper

Besoni apo jo, ideja e një virusi kompjuterik u parapriu rrjeteve kompjuterike. Matematikani John von Neumann parashikoi idenë në fund të viteve 1940, por vetëm 30 vjet më vonë, dikush krijoi një të tillë. Gjatë epokës së ARPANET (interneti në formën e tij më të hershme- fillestare) në 1971, pak përdorues të rrjetit u habitën kur në ekranet e tyre shfaqet fraza: "Unë jam kacavjerrësi, më kapni nëse mundeni." Në atë kohë, përdoruesit nuk kishin ide se kush ose çfarë mund të ishte. Creeper ishte një krimb, një lloj virusi kompjuterik që replikohet dhe përhapet në sisteme të tjera; u krijua nga Bold, Beranek dhe Newman. Ndryshe nga viruset me qëllim të keq që hasim sot, gjithçka që bëri Creeper ishte shfaqja e mesazheve. [2]

2.1.2. 20 shtator 1983 - Patenta e parë amerikane për sigurinë kibernetike

Ndërsa kompjuterët filluan të evoluojnë, shpikësit dhe ekspertët e teknologjisë në të gjithë botën po nxitonin të bënin histori dhe të pretendonin patenta për sistemet e reja kompjuterike. Patenta e parë amerikane për sigurinë kibernetike erdhi në shtator të vitit 1983 kur MIT u dha patentë amerikane 4,405,829 për një "sistem dhe metodë të komunikimit kriptografik". Patenta prezantoi algoritmin RSA (Rivest-Shamir-Adleman), i cili ishte një nga kriptosistemet e para me çelës publik. Kriptografia është themeli i sigurisë moderne kibernetike. [2]

2.1.3. 9 qershor 1993 - Konferenca e Parë DEF CON

DEF CON është një nga konferencat teknike më të njohura të sigurisë kibernetike në botë. Kjo konferencë ka filluar të mbahet në qershor të vitit 1993 nga Jeff Moss, u mbajt në Las Vegas me afërsisht 100 persona. Sot në konferencë marrin pjesë mbi 20,000 profesionistë të sigurisë kibernetike nga e gjithë bota. [2]

2.1.4. Shkurt 1995 – Krijimi i Shtresës së Soketeve të Sigurta (SSL) 2.0

Protokoli i sigurisë që lejon njerëzit të bëjnë gjëra të thjeshta si blerja e artikujve në internet në mënyrë të sigurt, u bë i mundur nga protokoli Secure Sockets Layer (SSL). Netscape filloi zhvillimin e protokollit SSL jo shumë kohë pasi që Qendra Kombëtare për Aplikacione me Super-procesim lëshoi shfletuesin e parë në internet. Në shkurt 1995, Netscape lëshoi SSL 2.0, i cili u bë thelbi i gjuhës për përdorimin e sigurt të internetit, i quajtur Protokoli i Transferimit të Hyper Text Secure. Sot, kur shihni "HTTPS" në një adresë në faqen e internetit, e dini që komunikimet e tij me shfletuesin tuaj janë të koduara. [2]

2.1.5. 1 tetor 2003 – Lindja e Anonymous

Anonymous ishte grupi i parë i hakerëve i njohur botërisht. Grupi nuk ka udhëheqës dhe përfaqëson shumë përdorues të komunitetit aktiv dhe pasiv në internet. Së bashku, ata ekzistojnë si një tru global anarkik, i dixhitalizuar. Duke veshur maskën e Guy Fawkes, grupi fitoi vëmendjen gjithë kombëtare atëherë kur pushtoi faqen e internetit të Kishës së besimit “Scientology” me

sulme të distribuuara DDoS. Anonymous vazhdojnë të jenë të lidhur me incidente të shumta të profilit të lartë, shkaku kryesor i veprimtarisë së tyre është mbrojtja e privatësisë së qytetarëve. [2]

2.1.6. 12 janar 2010 - Operacioni Aurora zbulon një komb-si-haker

Para vitit 2010, zbulimi i shkeljeve të sigurisë u konsiderua shumë i pazakontë. Më 12 janar të atij viti, Google tronditi botën kur njoftoi "Operacionin Aurora", një shkelje e madhe në infrastrukturën e saj në Kinë. Google fillimisht mendoi se qëllimi i sulmuesve ishte të hynin në llogaritë Gmail të aktivistëve kinezë të të drejtave të njeriut. Analistët zbuluan se qëllimi i vërtetë ishte identifikimi i operuesëve të inteligjencës kineze në SHBA, të cilët mund të kenë qenë në listat e vëzhgimit për agjencitë amerikane të zbatimit të ligjit. Sulmet goditën gjithashtu më shumë se 50 kompani në internet, financa, teknologji, media dhe sektorë kimikë. [2]

Në vitet e fundit, shkeljet masive kanë goditur markat e emrave si Target, Anthem, Home Depot, Equifax, Yahoo, Marriott dhe duke vënë në dorë shumë të dhëna kompromentuese për kompanitë dhe miliarda konsumatorë. Si reagim, u bën rregulloret më të rrepta për të mbrojtur privatësinë e qytetarëve si Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave të BE-së (GDPR) dhe “Akti i ri i Konsumatorit për Konsumatorin në Kaliforni” që po ngrit nivelin e pajtueshmërisë. Ndërsa, hapësira kibernetike është bërë një fushë beteje dixhitale për shtetet-kombet dhe haktivistët. Për të vazhduar, industria e sigurisë kibernetike po inovon vazhdimisht dhe po përdor mësime të përparuara makinerike dhe qasje të drejtuara nga Inteligjenca Artificiale - AI, si për shembull, për të analizuar sjelljen e rrjetit dhe për të parandaluar që kundërshtarët të fitojnë. [2]

Kur telefoni ishte ende një risi, ai ishte i lidhur fizikisht në shtëpi dhe mbase ishte vendosur në një cep të ndërtuar në mur. Në mënyrë të ngjashme, kabinat telefonike publike u ndërtuan për privatësi të telefonatës. Edhe bankat e telefonave me pagesë në hollet e hotelit ishin të pajisura me pengesa të zhurmës për të dhënë iluzionin e privatësisë. Me telefonat mobil, kjo ndjenjë e privatësisë është zhdukur tërësisht. Është e zakonshme të ecësh në rrugë dhe të dëgjosh njerëz që flasin me zë të lartë ndonjë dramë personale, ose më keq duke recituar numrin e kartës së tyre të kreditit para të gjithë atyre që kalojnë aty. Në mes të kësaj kulture të hapjes dhe ndarjes, ne duhet të mendojmë me kujdes për informacionin që po shpërndajmë vullnetarisht për botën.

Supozoni se ju pëlqen të punoni në kafenenë në qoshe të shtëpisë tuaj, e cila ka Wi-Fi falas. Kjo duhet të jetë në rregull, apo jo? Më vjen keq ta them, por jo. Wi-Fi publik nuk u krijua duke pasur

parasysh tregtinë elektronike. Ishte thjesht i përshtatshëm dhe është gjithashtu tepër i pasigurt dhe jo e gjithë ajo pasiguri është teknike. [5]

Seriozisht, nëse keni vërtet diçka të ndjeshme për të bërë larg shtëpisë tuaj, atëherë rekomandohet që të përdorni lidhjen celulare në pajisjen tuaj të telefonit në vend që të përdorni rrjetin Wi-Fi në aeroport ose në kafene. Ju gjithashtu mund të lidhni pajisjen tuaj personale mobile duke përdorur USB, Bluetooth ose Wi-Fi. Nëse përdorni Wi-Fi, atëherë sigurohuni që të konfiguroni sigurinë WPA2. Opsioni tjetër është të blini një port Hotspot për ta përdorur kur udhëtoni. Vini re gjithashtu, kjo nuk do t'ju bëjë të padukshëm, por është një alternativë më e mirë sesa përdorimi i Wi-Fi publik. Por, nëse keni nevojë të mbroni privatësinë tuaj nga operatori celular, për të shkarkuar të dhëna të ndjeshme - atëherë unë ju sugjeroj të përdorni HTTPS, kudo ose një Protokol të Sigurt të Transferimit të Skedarëve (SFTP). SFTP mbështetet në përdorimin e aplikacionit Transmit në Mac dhe aplikacionit Tunnelier në Windows. [5]

Daniel Buentello, një studiues i pavarur i sigurisë, njëri nga katër prezantuesit që folën për piraterinë e pajisjes në konferencën “Hulumtuesit në Black Hat USA 2014”, një konferencë për njerëzit në industrinë e sigurisë së informacionit, tha: Ky është një kompjuter që përdoruesi nuk mund të aktivizojë një antivirus. Më keq akoma, është si një derë sekrete e pasme që një person dashakeq mund ta përdorë dhe të qëndrojë aty përgjithmonë. “Është sikur një mizë në mur. ” [5]

Siç kemi parë, ndarja e jetës reale dhe jetës anonime në internet është e mundur, por kërkon vigjilencë të vazhdueshme.

Ndërsa koha kalon, gjithnjë e më shumë njerëzit po mësojnë për rëndësinë e sigurimit të të dhënave të tyre në internet. Sulmet e fundit në rrjetet e mëdha sociale kanë bërë që shumë njerëz të vetëdijesohen për çështjet e sigurisë kibernetike. Sulmet më të fundit në Facebook, të cilat e bënë kompaninë të pranonte se gati 50 milionë përdorues ishin në shënjestër kanë bërë që të gjithë aktorët në industri të ri mendojnë strategjitë e mbrojtjes së të dhënave.

Në të vërtetë, pesë vitet e fundit kanë qenë të vrullshme për përdoruesit e internetit. Ka pasur shumë sulme të profilit të lartë ndaj institucioneve financiare, kompanive të mediave sociale, blogjeve personale dhe shumë llojeve të tjera të faqeve të internetit. Në këtë periudhë gjithashtu është parë se sfera e sigurisë kibernetike evoluon në mënyrë drastike. Le të hedhim një vështrim se si fusha e sigurisë ka evoluar gjatë asaj kohe.

2.1.7. Gjendja e Sigurisë Kibernetike në vitin 2015

Në vitin 2015, Departamenti i Teknologjisë së Informacionit në Karolinën e Veriut dha statistika që tregojnë se sulmet kibernetike të synuara ndaj individëve dhe organizatave nuk ishin të rralla. Në të vërtetë, statistikat treguan se 80% e sulmeve të suksesshme ishin bërë duke shfrytëzuar njohuritë paraprake. Ishte një situatë e njëjtë diku tjetër ku sulmet nuk ishin saktësisht të sofistikuara. Sulmet e tilla do të parandaloheshin lehtë nëse njerëzit do të vetëdijesoheshin për mirësjellje dhe përdorimin e duhur të internetit.

Sado të thjeshta që ishin, sulmet e vitit 2015 inkurajuan ekspertët e sigurisë kibernetike të vinin më shumë theks në inkurajimin e njerëzve për të mësuar në lidhje me këshillat dhe praktikat e thjeshta të përdorimit të internetit. [6]

2.1.8. Rritja e kompleksitetit të kërcënimeve

Siguria kibernetike ka evoluar si rezultat i zhvillimit të kërcënimeve. Për një kohë të gjatë, kërcënimet kibernetike ishin të kufizuara në sulmet bazike që synim kishin vetëm një pajisje kompjuterike. Ndërsa në vitet e fundit, kërcënimet janë bërë më të avancuara dhe tani ato synojnë më shumë pajisje dhe më shumë rrjete gjithashtu. Siguria kibernetike ka evoluar për të siguruar që shkathtësitë janë pjesë e strategjisë së mbrojtjes. Shumica e organizatave nuk po mbështeten më në metodat reaktive kur bëhet fjalë për trajtimin e sulmeve. Siç është vërejtur nga Gobestvpn, organizatat e mëdha po formulojnë zgjidhje në kohë reale për sulmet. Kjo është konsideruar veçanërisht kohët e fundit kur sulmet kanë provuar se janë fatale për organizatat. Organizata të tëra janë detyruar të nënshtrohen nga kërcënime të mëdha të komplikuara. [6]

2.1.9. Ndryshimi i praktikave nga Organizatat

Në vitet e para të sigurisë kibernetike, detyra e sigurimit të rrjeteve iu la departamentit të Informacionit dhe Teknologjisë. Secila organizatë kishte një departament të denjë TI-së që kontrollonte rrjetet dhe kryente detyra të thjeshta si instalimi i programeve të sigurisë. Rritja e kërcënimeve ka detyruar organizatat moderne të ri mendojnë qasjen e tyre. Duke marrë parasysh se si inteligjenca e kërcënimeve kibernetike është thelbësore për të pasur një sistem të fuqishëm të sigurisë, çdo departament tani është i përfshirë në procesin e sigurisë kibernetike. [6]

2.1.10. Siguria kibernetike është bërë çelësi i inovacionit

Siguria kibernetike gjithashtu ka evoluar ndjeshëm në një pikë ku tani po udhëheq inovacionin. Ndërsa çështjet e sigurisë ishin të vogla në të kaluarën, ato tani janë bazë e të gjitha vendimeve që merren në botën e teknologjisë. Si rezultat i kërkimit për të shmangur sulmet në mënyrë të shpejtë, siguria kibernetike ka lejuar zhvillimin e sistemeve më të shpejta, më të fuqishme dhe pa probleme. Kjo, nga ana tjetër, ka paralajmëruar një epokë të re ku tani është i mundur zhvillimi i nivelit të ardhshëm të produkteve teknologjike. Ndërsa rrjetet forcohen, ne do të shohim më shumë evolucion në fushën e internetit të gjërave (IoT). Kjo në fund të fundit do të sjellë evolucion të paparë në industrinë e teknologjisë në tërësi. [6]

2.1.11. Gjendja e Sigurisë Kibernetike në 2018

Të gjitha zhvillimet që kanë ndodhur në disa nga vitet e fundit na kanë përgatitur për të tashmen. Tani jemi në një fazë ku sistemet janë shumë më të besueshme sesa ishin disa vite më parë. Sistemet më të shpejta, më të mençura dhe më të fuqishme kanë bërë të mundur që subjekte të ndryshme në fushën e sigurisë të përdorin me efikasitet të dhënat e mbledhura. Përfshirja e të dhënave në luftën kundër sulmeve ka ripërcaktuar përfundimisht atë që ka të bëjë me sigurinë kibernetike. Në ditët e sotme, raportet që vijnë nga sfera kibernetike kanë të bëjnë më shumë me njohuritë sesa me analiza të thjeshta. Kjo pasi të dhënat luajnë një rol të rëndësishëm në përmirësimin e inteligjencës. [6]

2.1.12. Zbulimi i politikës së sigurisë kibernetike

Çfarë është "siguria kibernetike" dhe si lidhet me politikën e sigurisë? Larg nga pranimi i një përgjigje të drejtpërdrejtë, kjo pyetje qëndron në zemër të debateve politike dhe akademike lidhur me këtë çështje. Së pari, siguria kibernetike është një term relativisht i ri për një sërë praktikash të vjetra rreth sigurisë së rrjeteve kompjuterike. [7]

Së dyti, përkufizimet për termin janë të kontestuara, të ilustruara nga refuzimi i disa aktorëve shtetërorë për të rënë dakord mbi një fjalor të përbashkët. [8]

Së treti, kuptimi i termit po ndryshon me kalimin e kohës. Jo shumë kohë më parë, një rreth i kufizuar i ekspertëve diskutuan sigurinë kibernetike kryesisht si një çështje e menaxhimit të

rreziqeve teknike në mbrojtjen kritike të infrastrukturës së informacionit. Tani qarqet më të larta qeveritare merren me sigurinë kibernetike si një sfidë kryesore e sigurisë kombëtare. [9]

Së katërti, paralel me përparimin e dixhitalizimit, gjithnjë e më shumë të aspekteve të ekonomisë, shoqërisë dhe politikës, shqetësimet e sigurisë kibernetike po zgjerohen në fusha shtesë të politikave. [10]

Si përmbledhje, siguria kibernetike është në të njëjtën kohë duke lëvizur lart në agjendën politike dhe duke u zgjeruar krahas si një problem në një mori fushash të politikave shtesë. Përkufizimet e thjeshta dhe statike nuk janë të përshtatshme për t'u marrë me kontekste që ndryshojnë vazhdimisht. Mirëpo, vërejmë se pika e përbashkët e politikës së sigurisë kibernetike karakterizohet nga dy faktorë kryesorë: Së pari, nga teknologjitë dixhitale, posaçërisht përdorimi i tyre dhe keqpërdorimi nga faktori njeri në aspektin ekonomik, social dhe politik; dhe së dyti, duke i rezistuar shpesh procesit të negociatave shumë konfliktuale në mjediset zyrtare dhe joformale midis shtetit dhe burokracive të tij, shoqërisë dhe sektorit privat, drejtuar drejt përcaktimit të roleve, përgjegjësive, kufijve ligjorë dhe rregullave të pranueshme të sjelljes. Dimensioni i parë lidhet me përdorimin e një sërë teknologjish të dallueshme dixhitale dhe sesi këto teknologji janë të lidhura me koncepte më të gjera të ndryshimeve socio-ekonomike. [11]

Lidhja e ngushtë në mes të kompjuterëve dhe telekomunikimeve, integrimi i këtyre teknologjive në një sistem global multimedial dhe disponueshmëria e tyre me kosto të lirë në të gjithë botën është themeli për paralajmërimin e transformimeve të shumëfishta, të shpejta dhe konsekuente në prodhim, menaxhim, ndërveprim shoqëror dhe qeverisje [12] edhe pse mbetet të shihet se sa revolucionare do të jenë këto ndryshime.

Pyetjet më adekuate lidhur me politikën e sigurisë kibernetike në raport me teknologjitë dixhitale dhe karakteristikat e tyre, cilat veprime i mundësojnë dhe cilat i ndalojnë ato, por gjithashtu kush i zhvillon, në çfarë mënyre, si, pse dhe kush ka fuqinë të i japë formë përdorimit dhe keqpërdorimit të tyre.

Dimensioni i dytë lidhet me rolin e shteteve dhe angazhimin e tyre me aktorë të tjerë në rang kombëtar dhe ndërkombëtar. "Siguria" në politikën e sigurisë kibernetike mund të lexohet në dy mënyra: Si politikë e sigurisë kibernetike (aspektet politike të sigurisë së çështjes), ose si politikë e sigurisë kibernetike (politika që përfshin çështjet e sigurisë kibernetike më gjerë). Kjo paqartësi

është e qëllimshme sepse ne e konsiderojmë si thelbësore pyetjen se çfarë lloji i politikës shfaqet nën çfarë lloj rregullash dhe me çfarë lloj kufijsh. [13]

Nga pikëpamja teorike, pyetja se sa politikë ka ose duhet të ketë në siguri - dhe sa siguri në politikë - na lejon të lidhim kërkimin në sigurinë kibernetike me debatet në studimet e sigurisë. [14]

E rëndësishme është gjithashtu se, shteti ka role të ndryshme në sigurinë kibernetike, duke filluar nga garantuesi i sigurisë, ligjvënësi dhe rregullatori, për të kërcënuar aktorin dhe rrezikun për shoqërinë dhe shtetet e tjera. [10]

Prandaj, politika e sigurisë kibernetike përcaktohet nga proceset e negociatave kombëtare dhe ndërkombëtare në lidhje me kufijtë e përgjegjësive të aktorëve shtetërorë, ekonomikë dhe shoqërorë, si dhe marrëveshja ose mosmarrëveshja mbi mjetet që përdorin këta aktorë. Ky dimension i dytë përfshin projeksionin e fuqisë nga aktorë të caktuar, si kontrolli mbi popullatat dhe flukset e informacionit dhe kthimin e tij prapa, gjithashtu. [13]

2.1.13. E Ardhmja e Sigurisë Kibernetike

Nuk ka dyshim se kryesit e krimeve kibernetike do të vazhdojnë të krijojnë mënyra të reja për të sulmuar organizata dhe individë. Bota e sigurisë kibernetike do të vazhdojë të zhvillohet gjithashtu. Ndërsa ekspertët do të vazhdojnë të krijojnë sisteme më të shpejta, puna më e rëndësishme tani në këtë fushë do të jetë sigurimi i informacionit. Shumë rrjete ende bien nga praktika të thjeshta, të cilat mund të shmangen nëse më shumë njerëz vetëdijesohen për këshillat themelore të sigurisë.

Figure 3. E ardhmja e sigurisë kibernetike[2]

[2] Burimi: https://www.alumni.pace.edu/s/1655/images/gid2/editor/2020/ar_virtual_events/futeur_of_cybersecurty.png

2.2. Puna nga distanca dhe zhvillimi i saj përgjatë historisë

Puna në distancë nuk është një shpikje "e re", por ekziston për rreth 1.4 milionë vjet më parë. Sigurisht, të gjithë po flasin për punë në distancë dhe fleksibilitet në kohë tani, mirëpo në çdo kohë të historisë njerëzore, ka pasur një version të "punës nga shtëpia".

Në fillimet e “të punuarit – punës”, nuk kishte asgjë të tillë siç është shkuarja në një vend tjetër për të punuar.

Njerëzit e hershëm kërkonin për të gjetur bimë dhe gjuanin kafshë për ushqim. Një nga më të hershmit ishte “Homo ergaster” i cili jetoi përgjatë Afrikës lindore dhe jugore midis 1.9 deri 1.4 milionë vjet më parë. Në kuptimin e plotë të fjalës, ai u emërua "njeriu që punon", këtë emër e mori për shkak që përdorte mjete të përparuara të punës. Provat nga kockat e kafshëve të djegura në depozitat fosile dhe gjurmët e kampeve të tyre tregojnë se ata i kanë punuar këto mjete afër vendbanimeve të tyre dhe kanë përdorur zjarrin.

2.2.1 Rrugëtimi i punës nga shtëpia, Mënyrat jo të mira të kombinimit të punës dhe shtëpisë

Shumë mijëvjeçarë më vonë, puna ishte grumbulluar në shtëpi. Anglia mesjetare kishte "shtëpinë e gjatë", e cila ishte e banuar nga fshatarë dhe bagëtia e tyre në të dy skajet e ndërtesës. Në mes, ishte kuzhina, si dhe qendra për tjerrje/ endje/ rrobaqepësi, qumështore, kasap, dhe rrezitje. Tregtarët mesjetarë gjithashtu punonin tregtinë e tyre nga shtëpia. [15]

Nuk ndryshoi shumë me kalimin e kohës. Siç dëshmohet nga ndërtesat më e vjetër se 200 vjeçare me dritare të mëdha që ekzistojnë ende në Angli, artizanët e shekullit XVII dhe XVIII, të tillë si endësit e mëndafshit dhe orëndreqësit, përdorën bollëkun e dritës natyrore për të bërë prodhimet e tyre. Disa shtëpi pune të quajtura "dyqane të shkëlqyera" kishin një "motor me avull në njërin skaj dhe një bosht të vetëm drejtues që lidhte rrymat elektrike në pallatet individuale të endjes" për t'i lejuar ata të konkurrojnë me fabrikat. [15]

Gjithashtu vërejmë se pas Revolucionit Industrial, puna në shtëpi vazhdoi të lulëzonte pasi dyqanxhinjtë, sallonet e varrimit dhe shkollat kishin pronarë dhe mësues që jetonin dhe punonin në të njëjtën ndërtesë. [15]

2.2.2 Shitja në shtëpi dhe shpikja e "Telekomunikimit"

Gjatë Luftës së Dytë Botërore filloi ngritja e vendeve të punës për gratë, ndërsa, koha e paqes i ktheu përsëri në shtëpitë e tyre. Në këtë pikë, ndodhën dy risi: njëra ishte shpikja dhe prodhimi i kontejnerëve plastikë për të ruajtur ushqime dhe mallra të tjerë duke përdorur një nënprodukt industrial të krijuar nga Earl Tupper; Tjetra ishte mënyra për t'i shitur ato, krijuar nga Brownie Wise, një grua që do të bëhej shitëse e produkteve të pastrimit të Stanley Home. Ajo u tërhoq nga modeli i partisë Stanley Home dhe krijoi "partinë e saj" si një mënyrë për t'i bërë amviset të provonin produktet dhe të argëtoheshin ndërsa e bënin atë. Kjo shpiku një industri të tërë të shitjeve në shtëpi. [15]

Kujtojeni që në fillimin e viteve 1970 erdhi kriza e naftës, krahas ngritjes së çështjes së përdorimit të makinave për të udhëtuar nga periferitë në zyrat e tyre në qytet. Mirëpo, përparimi i mëtejmë i teknologjisë i lejoi punëtorët të përdorin shtëpitë e tyre për një qëllim të dyfishtë. [15]

Kjo ndodhi kur Jack Nilles ishte duke punuar në distancë në një sistem kompleks të komunikimit të NASA-s, i cili krijoi fjalën "telekomunikim". Ai vazhdoi me bashkë-autorin e Telekomunikacionit-Transportit Tradeoff, i cili propozoi të punonte nga shtëpia si një zgjidhje për ngatërresat e trafikut si dhe burimeve të kufizuara. [15]

2.2.3 Puna në distancë dhe orët fleksibile

Në vitet 1980, kompanitë filluan zyrtarisht të eksperimentojnë me orarin fleksibil. Për shembull, IBM instaloi "terminale të largëta" në shtëpitë e disa punonjësve gjatë asaj kohe dhe programi lulëzoi deri në atë pikë sa që "deri në vitin 2009, 40% e 386,000 punonjësve globalë të IBM-it tashmë kishin filluar punën nga shtëpia (kompania vuri në dukje se kishte zvogëluar hapësirat për zyre në SHBA me 78 milionë metra katrorë dhe si rezultat kursente rreth 100 milionë dollarë çdo vit)", citon një raport në Quartz. [15]

Deri në vitin 2010, Qeveria kishte miratuar Aktin e Rritjes së Telework, i cili u përpoq të bënte telekomunikimin më të sigurt dhe efektiv për punonjësit federalë. Raporti më i fundit i regjistrimit

zbuloi se 13.4 milionë njerëz (nga një fuqi punëtore prej 142 milionë) punonin nga shtëpia, e cila përfaqësonte një rritje prej 4.2 milionë në pak se një dekadë. [15]

Puna në distancë vazhdon të lulëzojë. Një raport i fundit nga FlexJobs tregon se kompanitë në të gjithë sektorët e industrisë po ofrojnë orare fleksibile të punës dhe disa pozicione paguhen me gjashtë shifra. Gjithashtu, mos të harrojmë ngritjen punës së pavarur profesionale. Një studim i fundit, në vitin 2014 nga Unioni Upwork dhe Freelancer zbuloi se në mijëvjeçarin e tanishëm demografia më e madhe në fuqinë punëtore amerikane, 42% e të rinjve 18 - 34 vjeç, tani punojnë të pavarur. [15]

"Nuk ka topa kristali, por një mënyrë e mirë për të vlerësuar të ardhmen është të shohësh njerëzit që e trashëgojnë atë," shkruan Stephane Kasriel, CEO i Upwork. “Shumë nga ata që zgjedhin të punojnë ndryshe sot po e bëjnë këtë për t'u kthyer në gjërat themelore dhe më afër jetës që duan. Për ta arritur atë, njerëzit kanë nevojë për fleksibilitet për të përcaktuar jetën e tyre sipas kushteve të tyre." [15]

2.2.4 Historia, evoluimi dhe e ardhmja e punës në distancë. Si arritëm deri këtu?

Puna në distancë nuk është gjë e re, kohëve të fundit ka filluar të popullarizohet falë teknologjisë dhe ekspozimit nga etiketimet në rrjete sociale #shtegëtuesitdigjital dhe #punoprejçdovendi.

Në vitet 1980 kur fillimisht interneti u krijua, puna në distancë nuk ka lindur brenda natës. Terminologjia “Puna në distancë” ekzistonte shumë më parë se takimet në zyre dhe mbledhjet.

Para revolucionit industrial, të gjithë punonin nga shtëpia. Farkëtarët, zdrukthëtarët, punëtorët e lëkurës dhe poçarët ngritën dyqanet në vendbanimet e tyre dhe shisnin mallrat e tyre prej andej.

Me revolucionin industrial erdhi edhe nevoja për automatizimin dhe krijimin e fabrikave.

Makineritë e mëdha dhe prodhimet në shkallë të gjerë kërkonin që punonjësit të ishin të pranishëm për të përfunduar punën e tyre. Gjithashtu njerëzit filluan të udhëtonin në "hapësirat e zyrave" të caktuara.

Menjëherë pas Luftës së Dytë Botërore historia ndryshoi edhe më tej. [16]

Ndërsa ekonomia amerikane forcohej, kështu u rritën edhe zyrat qendrore të korporatave, hapësira më të mëdha për zyra dhe selitë e ndara të kompanisë. Dita e punës 8-orëshe lindi gjithashtu në të njëjtën kohë. [16]

Me këtë zgjerim ekonomik erdhën përparimet në teknologji dhe kompjuterët që hapën rrugën për punëtorët e sotëm në distancë, në mënyrën siç i njohim tani.

Shumë njerëz u pajisën me kompjuterë personal, duke i dhënë hapësirë në shtëpitë e tyre "Rrjetit të Gjerë Botëror" (World Wide Web),dy ngjarje që më vonë i shtruan rrugën punës në distancë janë, Interneti Publik dhe Rrjeti pa tela. [16]

Qoftë duke punuar nga një zyrë shtëpie, laptop në një kafene, apo edhe një telefon i mençur, interneti u dha punonjësve qasje në aplikacione të bazuara në Cloud të cilat i lejonin të bënin gjithçka që do të bënin në punishten e tyre, edhe prej jashtë zyrës.

Punonjësit virtualë punojnë gjatë gjithë ditës dhe mund të qëndrojnë në kontakt me bashkëpunëtorët e tyre nga e gjithë bota falë internetit. Pra, kjo është vetëm një arsye pse puna në distancë vazhdon të jetë kaq e popullarizuar.

Pra, Sa e zakonshme është puna në distancë këto ditë? Sipas një studimit të Gallup, "43 përqind e amerikanëve të punësuar thanë se kaluan të paktën disa kohë duke punuar në distancë. [16]

Meqenëse punëtorët në largësi i kryejnë detyrat e tyre të punës jashtë zyrës dhe zakonisht në oraret e tyre, ata gjithashtu kanë tendencë të kenë nivele më të larta angazhimi dhe gjithashtu rritje të niveleve të produktivitetit, prandaj kjo i bën ata kandidatë tërheqës për punësim.

"Njerëzit që kalojnë mes 60-80% të orëve të tyre të punës në distancë për të paktën 3-4 ditë të javës, raportojnë nivele më të larta të angazhimit në krahasim me ata që nuk punojnë kurrë jashtë zyrës." [16]

"Njerëzit që punojnë nga shtëpia përfundojnë 13.5% më shumë detyra sesa personeli në zyrë", që doli të ishte një punë tjetër me vlerë një ditë të plotë, sipas një studimi tjetër rasti.

Shumica e punëtorëve në distancë nuk kanë synim të largohen për në kullota më të gjelbërta. Kjo do të thotë që kompanitë mbajnë norma më të larta të mbajtjes dhe harxhojnë më pak para duke trajnuar rekrutët e rinj. [16]

Dhe sapo punonjësit të kalojnë në punë në distancë, ata pothuajse kurrë nuk duan të kthehen pasi "90% e punëtorëve në distancë planifikojnë të punojnë në distancë për pjesën tjetër të karrierës së tyre." [16]

Ata janë kaq të kënaqur me këtë marrëveshje "94% e punëtorëve në distancë të anketuar thanë se ata inkurajuan të tjerët të punojnë në distancë. [16]

Punësimi i punëtorëve në distancë u jep kompanive avantazhe konkurruese si:

Shëndet më i mirë mendor dhe fizik për punonjësit. Ndërrimi i udhëtimeve stresuese për të arrit me kohë në punë me ushtrimet e mëngjesit. Prandaj, punonjësit kanë më shumë kohë për t'u përqendruar në shëndetin e tyre, gjë që mund të rrisë produktivitetin dhe ndjenjat e përgjithshme të lumturisë.

Përmirësimi i ekuilibrit punë-jetë. Meqenëse punëtorët në distancë kanë fleksibilitet më të madh në oraret e tyre, ata kanë kohë për familjen, detyrimet personale dhe karrierën e tyre. Dhe me më pak pauza, ato arrihen më shpejt.

Në përgjithësi, do të thotë se më shumë para mund të shpenzohen për aktivitetet e formimit të ekipit dhe të minimizohen linjat shtesë të telefonit, grickat për dhomën e pauzës dhe furnizimet e zyrës.

Me këto rezultate pozitive të punës nga distanca, është e lehtë të kuptosh pse menaxherët kanë 4 herë më shumë gjasa të punësojnë profesionistë të pavarur në vitin 2018.

Falë një pakoje mjetesh për të përmirësuar jetën e punës në distancë si për punonjësit ashtu edhe për punëdhënësit, nuk ka qenë kurrë më e lehtë të qëndrosh i lidhur dhe të realizosh më shumë punë së bashku. [16]

Teknologjia mban të lidhur punëtorët dhe punëdhënësit në distancë, sikurse përdorimi i Slack. Këtu çdokush në ekip mund të bashkëpunoj me punonjës të tjerë që punojnë në të gjithë globin po aq lehtë sa dërgimi i një mesazhi me tekst. [16]

Mjetet e menaxhimit të projektit si Trello krijojnë gjithashtu një listë dixhitale që e mban gjithë ekipin në një platformë bashkëpunuese, pavarësisht se nuk kanë qenë kurrë në të njëjtin vend fizik. Dhe thirrjet konferencë virtuale sigurojnë që askush të mos mbetet i huaj pas ekranit të kompjuterit. Bashkëpunimi në takimet “ballë për ballë” e mbajnë vendin virtual të punës më njerëzor. [16]

Me kaq shumë mënyra për të bashkëvepruar me njëri-tjetrin në internet, është sikur të gjithë në kompani po punojnë ende së bashku nën të njëjtën çati. Përveç se në mënyrë shumë më të mirë.

2.2.5 Si e transformoi teknologjia punën në largësi dhe çfarë ka e ardhmja

Kjo kronologji tregon se si teknologjia hapi dyert për punën në distancë dhe ndihmoi në formësimin e vendit virtual të punës që kemi sot:

1975: Prezantohet kompjuteri i parë "personal". Punonjësit më në fund janë në gjendje të punojnë në distancë jashtë zyrës dhe përfundimisht të marrin punën e tyre gjatë lëvizjes me një laptop ose tablet. [16]

1990: Lind interneti dhe World Wide Web që ndihmon në lidhjen e punëtorëve në distancë me postën elektronike dhe mjetet virtuale të zyrës. [16]

1990: Qeveria Federale kryen një studim për telekomunikimin që përfshinë mbi 2,000 punëtorë federalë. Njerëzit u treguan më produktiv, kishin një cilësi më të mirë të jetës dhe ekuilibrit të jetës në punë dhe shkurtuan shpenzimet dhe kohën e udhëtimit gjatë telekomunikimit. Punëtorët në distancë i kanë të njëjtat përfitime sot. [16]

1994-1995: Kompanitë si American Express, IBM dhe AT&T fillojnë të lejojnë punonjësit e tyre të punojnë nga distanca duke përdorur telekomunikimin. Duke pasur sukses të vazhdueshëm, ideja u përhap shpejt dhe u adaptua nga të tjerët. [16]

1997: Google lëshon makinën e fuqishme kërkuese që njohim sot. Google Search thyen barrierat dhe krijon një vend ku punëdhënësit dhe punonjësit mund të gjejnë njëri-tjetrin pa marrë parasysh se ku jetojnë. Mund të gjesh akoma punë të largëta ose punëtorë në çdo kohë sot, të gjitha nga kryerja e një kërkimi të thjeshtë në Google. [16]

1999: Mjetet e centralizuara të menaxhimit të projektit si Basecamp u japin menaxherëve dhe punonjësve një vend të centralizuar për të menaxhuar rrjedhat e punës në distancë. Kjo i mban të gjithë në të njëjtën platformë pune, pavarësisht se jetojnë në zona të ndryshme, sidomos kur bëhet fjalë për afatet dhe projektet e filluara. Mbi 100,000 kompani ende e përdorin këtë softuer të menaxhimit të projektit. [16]

Vitet 2000: Interneti pa tela dhe brezi i gjerë. Punonjësit në distancë më në fund mund të punojnë pa u lidhur me një vendndodhje fizike për lidhjen e tyre të internetit ethernet. [16]

2002: Linkedin fillon dhe lidh miliona profesionistë në të gjithë globin. Ju ende mund të krijoni rrjete me miq të vjetër ose bashkëpunëtorë, të kontaktoni me punëdhënësit e mundshëm dhe të ndiqni kompanitë tuaja të preferuara për të parë se çfarë ka të re në këtë platformë profesionale që mburret me 562 milionë përdorues në 200 vende dhe territore. [16]

2003: Një rritje të punonjësve në distancë e frymëzon edhe Skype, një mjet më i mirë komunikimi për punonjësit virtualë. Ky program video konferencë ndihmon organizatat të mbajnë lidhje të drejtpërdrejta ballë për ballë me punonjësit edhe nëse të gjithë punojnë në distancë. Përdoruesit e tij e përdorin shumë edhe në intervista të largëta për të vendosur një fytyrë dhe personalitet për secilin kandidat pas ekranit. [16]

2004: Softueri i takimit virtual GoToMeeting (GTM) i ndihmon punonjësit të "takohen" në një dhomë konferencash virtuale për të ndarë prezantimet, skedarët dhe mendimet së bashku. GTM aktualisht ka 2 milionë përdorues aktivë të përditshëm. [16]

2006: Softueri për ndjekjen e kohës Toggl e bën më të lehtë për punonjësit të paraqesin fletat e punës në agjendë kohore pa shumë përpjekje. Kjo i ndihmon punëtorët në distancë të ndjekin orët e tyre të punës dhe të paguhen në përputhje me rrethanat. [16]

2009: Slack, i cili është gjithashtu aplikacioni i biznesit me rritjen më të shpejtë në histori, i cili krijon një mënyrë që shokët e ekipit dhe menaxherët të komunikojnë nga kudo. Ai mbështet 8 milionë përdorues aktivë të përditshëm dhe ka mbi 70,000 klientë që e paguajnë. [16]

2012: Google prezanton paketën e saj të mjeteve të zyrës dhe ruajtjen e skedarëve dixhitalë, të njohur si Google Drive. Kjo bëhet hapësira e punës e ditëve moderne, ku punonjësit, si brenda zyrës dhe në distancë, kanë qasje në dokumente dhe skedarë të rëndësishëm ndërsa bashkëpunojnë dhe reagojnë në kohë reale. [16]

2016: Dell raporton një kursim vjetor prej 12 milionë dollarë që nga zgjerimi i programeve të tij të telekomunikimit dhe punës në distancë. Raporte si këto provojnë se puna në distancë është e dobishme për punëdhënësit po aq sa edhe për punonjësit në distancë. [16]

2017: Qytetet kryesore të mëdha me teknologji si Austin dhe San Francisco raportojnë se 60% dhe 30% e ofertave të tyre të punës u shkuan punëtorëve në distancë. Tani shumë punëdhënës preferojnë të zgjedhin punonjësin më të talentuar, edhe nëse kjo do të thotë të dalin jashtë zonës gjeografike të korporatës për ta bërë këtë. [16]

2018 dhe më tej: "4.3 milionë njerëz aktualisht punojnë nga shtëpia në Shtetet e Bashkuara, të paktën gjysmën e kohës" dhe kjo shifër është rritur 150% në 13 vitet e fundit. E ardhmja e punës në distancë vazhdon të shpërthejë dhe teknologjia për të mbështetur këto nevoja vetëm po avancohet. [16]

Tabela 1. Rritja e punës nga distanca dhe ngjarjet e TI-së ndër vite[3]

Viti	Ngjarja	Përqindja
1975	Kompjuteri i parë "personal"	1%
1990	Interneti dhe World Wide Web	7%
1990	Telekomunikimi që përfshinë mbi 2,000 punëtorë federalë	7.3%
1994-1995	Kompanitë si American Express, IBM dhe AT&T fillojnë të lejojnë punonjësit e tyre të punojnë nga distanca	13.7%
1997	Google lëshon makinën e fuqishme kërkuese Google Search	18.3%
1999	Mjetet e centralizuara të menaxhimit të projektit si Basecamp	20.6%
2000	Interneti pa tela dhe brezi i gjerë	23.7%
2002	Linkedin	24%
2003	Skype	25.3%
2004	GoToMeeting (GTM)	25.7%
2006	Toggl	28.7
2009	Slack	29%
2012	Google Drive	35%
2016	Dell raporton për programet e tij të telekomunikimit dhe punës në distancë	43%
2017	Qytetet, si Austin dhe San Francisco raportojnë ofertat e tyre të punës së punëtorëve në distancë	45%

[3] Burimi: https://weworkremotely.com/history-of-remote-work

2018	3 milionë njerëz aktualisht punojnë nga shtëpia në Shtetet e Bashkuara, të paktën gjysmën e kohës	60%

Intervista juaj e ardhshme e punës mund të bëhet përmes një bisede në Portalin Facebook që ju mund ta realizoni në dhomë, ose një iPad robotik që ju bën një vizitë në zyrën e intervistuesit sikur të qëndronit aty personalisht.

Është më e lehtë për të gjetur punë në distancë këto ditë. Pra, nëse e keni menduar ndonjëherë punën në distancë, tani është koha të bëni një gjë të tillë, edhe nëse filloni vetëm me kohë të pjesshme.

Prova është e qartë: Puna në distancë është këtu për të qëndruar!

Edhe pse punëtorët në distancë të ditëve të para-Revolucionit Industrial mund të mos kenë asgjë të përbashkët me punëtorët në distancë të sotëm, është një fakt se puna në distancë ka qenë duke u zhvilluar në heshtje që nga fillimi i fuqisë punëtore siç e njohim ne. Dhe meqenëse përfitimet janë më të mëdha se dëmet, puna në distancë nuk tregon shenja të venitjes. [16]

Falë përparimeve në teknologji, të cilat vetëm vazhdojnë të bëhen më të mira dhe më të shpejta, do të bëhet më e lehtë për punonjësit të punojnë në distancë dhe të bashkëpunojnë virtualisht - dhe punëdhënësit të punësojnë më shumë prej tyre. [16]

Por, kjo gjithashtu do të thotë që të dy palët do të duhet të përshtaten me ndryshimin e kohës.

Punonjësit do të duhet të ndihen rehat me mjetet e largëta dhe të kenë disiplinën e kërkuar për të qenë produktivë jashtë zyrës. Pa zotëruar këto aftësi thelbësore, puna në distancë nuk do të jetë aq e këndshme ose e frytshme. Dhe punëdhënësit të cilët krijojnë politika që promovojnë punën në distancë duhet të nxisin një mjedis që siguron që punonjësit virtualë të lulëzojnë. Bërja e kësaj do të tërheqin gjithashtu talente të shumët nga e gjithë bota. [16]

2.3 Ndikimi i COVID19 në Sigurinë kibernetike

Siç e dimë, shoqëria po përjeton një nga pandemitë më të këqija të këtij shekulli. Pandemia COVID19 ka pasur një ndikim masiv në botë dhe disa vende ka bllokuar dhe vendosur tashmë në një ngërç. Ndikimi i gjerë i pandemisë COVID19 në jetët e biliona njerëzve në botë ka krijuar atë që zakonisht do të mund të i referoheshim me “Realiteti ynë i ri” në normat tona shoqërore dhe

mënyrën e të jetuarit dhe të punuarit. Gjatë këtyre kohërave, siguria kibernetike ka pasur edhe më shumë rëndësi, pasi që kriminelët kibernetikë kanë pasur mjedisin e duhur për të sulmuar. Gjatë kësaj pandemie, shoqëria ka parë një rritje masive në frontin e sulmeve të sigurisë kibernetike.

Ndikimi i COVID19 në shoqëri, nga perspektiva e kërcënimit të sigurisë kibernetike ka dhënë gjithashtu edhe një diskutim mbi arsyen pse edukimi mbi i sigurinë kibernetike është ende i një rëndësie të madhe. Vetëdijesimi, si gjithmonë, duket se është mjeti numër një se si të parandalohen kërcënimet e sigurisë kibernetike.

Bota siç e dimë nuk do të jetë kurrë e njëjta. Fillimi i vitit 2020 solli diskutime në lidhje me familjen e viruseve koronavirus dhe si ato po ndikojnë në jetën tonë të përditshme. [17] COVID19 kishte një ndikim masiv në shoqërinë si tërësi në fillim të vitit 2020. Virusi u identifikua për herë të parë në Wuhan, Hubei, Kinë në Dhjetor 2019. [18] Më pas, më 11 Mars 2020, virusi është klasifikuar si pandemi nga Organizata Botërore e Shëndetësisë (OBSH). [19]

I takon specialistëve të sigurisë kibernetike të bëjnë gjithçka për të mbrojtur publikun e gjerë si një shërbim publik, gjatë gjithë kësaj pandemie. [20] Tani ka një hov masiv të sulmeve të sigurisë kibernetike të cilat po bëhen çdo ditë kundër publikut të gjerë. [21] Diçka duhet të bëhet në lidhje me të, megjithatë, mund të jetë tashmë tepër vonë. Siç kanë përmendur disa artikuj në të kaluarën, edukimi është thelbësor, vigjilenca e sigurisë kibernetike ende mungon masivisht në publikun e gjerë. [22] Dikush mund të argumentojë gjithashtu, nëse bota ishte me të vërtetë e përgatitur për virusin "njerëzor", dhe sinqerisht në situatën aktuale duket sikur të mos ishim përgatitur kurrë për COVID19. [23]

2.3.1 Përhapja e keqinformimit

Keqinformimi është një nga armiqtë më të mëdhenj të shoqërisë gjatë kësaj pandemie. Meqenëse vetë publiku po bën një punë mbresëlënëse duke shpërndarë lajme të rreme mes vete, kriminelëve kibernetikë u kërkohet vetëm të botojnë lajmet në një mënyrë të bujshme. Ka pasur një rritje masive të lajmeve të rreme dhe disa kompani po përpiqen në mënyrë aktive ta zgjidhin këtë [24], [25]. Rrjeti Njerëzit për Njerëzit (H2H) ka investuar 500 000 funte për të luftuar kundër keqinformimit [26].

2.3.2 Ueb-faqet me qëllime të këqija dhe sulmet e ardhshme

Një nga sulmet e para kibernetike në lidhje me COVID19 ishte në lidhje me hartat false të COVID19. Universiteti Johns Hopkins siguroi një nga hartat e para që përfshinte statistika për botën. Ky ka qenë një burim i shkëlqyer për shoqërinë dhe është provuar të jetë shumë i dobishëm. Sidoqoftë meqenëse ishte kaq i popullarizuar, sulmuesit kibernetikë krijuan versionet e tyre "false" të faqes që ju kërkonte përdoruesve të shkarkonin një shtojcë. Kjo shtojcë më pas do të lejojë që një sulmues të fitojë qasje në distancë në sistemin tuaj [27], [28].

Shembull tjetër kanë qenë uebfaqet të cilat maskoheshin si kanale zyrtare të komunikimit siç janë OBSH apo Qendra për Kontrollin e Sëmundjeve dhe u kërkonin përdoruesve të shkarkojnë dokumente që përmbanin këshilla të sigurisë. Më vonë është zbuluar se shumica e këtyre faqeve ishin me qëllime të këqija dhe fajllet që u shkarkuan përmbanin malware (viruse) të krijuar për të vjedhur kredencialet bankare ose për të bllokuar fjalëkalimet e njerëzve [27], [29].

Rëndësia e diskutimit të sulmeve të ardhshme është mënyrë për të përcaktuar si do të zhvillohen këto sulme dhe çfarë mund të bëjmë në të ardhmen. Fatkeqësisht, këto sulme nuk do të zhduken për një kohë të gjatë. Autorët parashikojnë se ato do të zhvillohen së bashku me evolucionin e pandemisë. Sugjerohet se shumë shpejt do të shohim edhe më shumë uebfaqe qëllim këqija, lajme të rreme dhe përpjekje për mashtrim.

2.3.3 Ndikimi dhe Parandalimi

COVID19 tashmë ka pasur një ndikim masiv në botë. Shoqëria ka shumë të ngjarë që kurrë të mos jetë e njëjtë pas kësaj, megjithatë, ne mund ta përdorim njohurinë e marrë gjatë gjithë pandemisë për një të ardhme më të mirë. Për fat të keq, shoqëria jo gjithmonë i përgjigjet çdo paralajmërimi, pasi zakonisht ekziston qëndrimi indiferent ndaj shenjave paralajmëruese. Pandemia COVID19 është një shembull i shkëlqyeshëm i kësaj ashtu siç edhe Bill Gates e ka përmendur qartë në një nga bisedat e tij Ted se shoqëria siç e dimë nuk është e përgatitur për një shpërthim masiv të ndonjë virusi [23]. Ndikimi i COVID19 nga një perspektivë e sigurisë kibernetike do të ketë ndikim më së shumti në fushat e mëposhtme: keqinformim, krijimin e frikës, dezinformimin, bizneset, ekonominë dhe çështjet kibernetike. Ne nuk kemi qenë të gatshëm për COVID19 dhe ne kurrë nuk jemi përgatitur për të pasur një siguri kibernetike. Edukimi mbi

çështjet e sigurisë kibernetike duhet të jetë domosdoshmëri e çdo organizate. Ne nuk mundemi të kemi pritshmëri nga individët që të jenë vigjilent nëse ata nuk kanë njohuri bazike mbi teknologji. Edukimi është thelbi i këtij problemi, të gjithë punëtorët duhet të marrin trajnime se si të mbrojnë veten në Internet. Inxhinieria sociale herë pas here ka treguar se individi (punëtori në këtë rast) është pika më e dobët për sigurinë kibernetike në çfarëdo organizate. Punëtorët janë duke u ballafaquar me probleme të sigurisë kibernetike që nuk janë përballur kurrë më parë. Tani është shumë vonë për t'u përgatitur, megjithatë ne mund të fillojmë me parandalimin e menjëhershëm. Tani është koha për t'u drejtuar nga programuesit e sigurisë kibernetike, tashmë kemi shpenzuar kohë të mjaftueshme, duhet të përdorim kohën e mbetur me mençuri.

Që nga shpërthimi i pandemisë, ka pasur raporte për shtirje si persona të autoriteteve publike (p.sh. OBSH) dhe organizata (p.sh., supermarkete, linja ajrore) [30], [31], duke shenjëstruar platforma mbështetëse [32], [33], duke mashtruar me Pajisje të Mbrojtjes Personale (PPE) [34] dhe duke ofruar shërim për COVID19 [35], [36]. Këto mashtrime targetojnë anëtarë të publikut të përgjithshëm, po ashtu edhe miliona individë që punojnë nga shtëpia. Puna nga shtëpia në masë ka zbuluar një nivel tjetër të shqetësimeve dhe sfidave mbi sigurinë kibernetike që industria dhe popullata nuk është përballur kurrë. Kriminelët kibernetikë e kanë shfrytëzuar këtë mundësi të zgjerojnë sulmet e tyre, duke përdorur hile tradicionale [37] që gjithashtu ndikojnë në rritjen e stresit dhe ankthit. Përveç kësaj përvojat e punës në shtëpi zbuluan nivelin e përgjithshëm të pa përgatitjes nga zhvilluesit dhe ofruesit e softuerit, veçanërisht për sa i përket sigurisë së produkteve të tyre. Sulmet kibernetike kanë shenjëstruar infrastrukturat thelbësore siç janë shërbimet shëndetësore [38]. Në përgjigje të kësaj, me 8 Prill 2020, Qendra Kombëtare e Sigurisë Kibernetike e Mbretërisë së Bashkuar (NCSC) dhe Departamenti i Shteteve të Bashkuara të Sigurisë Kombëtare (DHS) Agjencia e Sigurisë Kibernetike dhe e Infrastrukturës së Sigurisë (CISA) publikuan një këshillim të përbashkët se si grupet e krimit kibernetikë dhe kërcënimet e vazhdueshme kibernetike po shfrytëzonin gjendjen aktuale me pandeminë COVID19 [39]. Ky këshillues shqyrtonte çështje siç janë mashtrimet, malware dhe rreziqet e platformave komunikuese (p.sh., Zoom, Microsoft Teams).

2.3.4 Sulmet kibernetike në Mbretërinë e Bashkuar gjatë COVID19

Shtrirja e problemeve të lidhura me sigurinë kibernetike në Mbretërinë e Bashkuar ishte mjaft e jashtëzakonshme dhe në këtë pjesë ne përdorim Mbretërinë e Bashkuar si një rast studimi për të analizuar krimin kibernetikë të lidhur me COVID19. Ky diskutim tregon se siç pritej dhe përshkruhej më sipër, kishte një lidhje reciproke të lirshme midis njoftimeve të politikave/lajmeve dhe fushatave të lidhura me krimin kibernetikë. Analiza e paraqitur këtu fokusohet vetëm në eventet e krimit kibernetikë që kanë ndodhur në Mbretërinë e Bashkuar. Kështu për shembull, edhe pse shumë nga incidentet e identifikuara në seksionin e mëparshëm dhe veçanërisht [40] sulmet kibernetike globale, diskutimi këtu i injoron ato. Si pasojë, njoftime të shumta që supozohet se vijnë nga organizata me reputacion të tillë siç është OBSH dhe një bollëk i mashtrimeve që arritën te qytetarët e Mbretërisë së Bashkuar injorohen pasi që këto nuk janë probleme specifike të Mbretërisë së Bashkuar. Indikacionet e shkallës së problemit të incidentit të krimit kibernetikë në Mbretërinë e Bashkuar të përjetuar gjatë pandemisë sigurohen nga niveli i dyshimeve të raportuara në postën elektronike dhe mashtrimet. Deri në fillim të majit (07.05.2020), ishin raportuar në Qendrën Kombëtare të Sigurisë Kibernetike [41] më shumë se 160,000 email-e 'të dyshuara' dhe deri në fund të majit (29.05.2020), 4.6 milionë funte ishin humbur nga mashtrimet e lidhura me COVID19 me rreth 11,206 viktima të fushatave të mashtrimit dhe mashtrimit [42]. Si kundërpërgjigje Qendra Kombëtare e Sigurisë Kibernetike mbylli 471 dyqane të rreme online [43] dhe HMRC (Të Ardhurat dhe Doganat e Madhërisë së Saj) mbylli 292 uebfaqe të rreme [44]. Afati kohor në Figurën 3 tregon një seri ngjarjesh specifike në Mbretërinë e Bashkuar dhe incidenteve të krimit kibernetikë. Afati kohor tregon një korrelacion të drejtpërdrejtë dhe të anasjelltë midis njoftimeve dhe incidenteve. Korrelacionet e drejtpërdrejta janë raste kur autorët duket se ndjekin njoftime ose ngjarje, ata mund të jenë tërhequr nga këto ngjarje dhe kanë konfiguruar me kujdes sulmet kibernetike rreth kontekstit të politikës. Këto janë treguar në figurë me një shigjetë lidhëse me ngjyrë të fortë. Korrelacionet e anasjellta janë raste kur një incident nuk ka ndonjë korrelacion të qartë me një ngjarje ose njoftim. Megjithëse korrelacionet e anasjellta nuk duket se kanë një korrelacion të drejtpërdrejtë, këto mund të ekzistojnë sepse një numër ngjarjesh po nënvizoheshin në mënyrë aktive në media. Për shembull, çështja e pajisjeve mbrojtëse personale (PPE) ishte në diskutim aktiv shumë më parë se qeveria e Mbretërisë së Bashkuar të merrte këtë përparësi në konsideratë.

Në mënyrë të ngjashme, gjasat e një skeme të zbritjes së taksave ishin në shqyrtim aktiv në fillim të Marsit para shpalljes së buxhetit në (11.03.2020). Fushatat e para të phishing për zbritjen e taksave ishin në qarkullim aktiv para njoftimit të buxhetit. Në të dy rastet, duhet të theksojmë se këto janë korrelacione të lira dhe duhet të punohet më shumë në lidhje me faktin nëse një model parashikues mund të ndërtohet duke përdorur këto të dhëna dhe të dhënat në të gjithë botën si shembuj. Më 11 Mars 2020, qeveria e Mbretërisë së Bashkuar bëri një numër njoftimesh të rëndësishme buxhetore që përfshinin: një fond reagimi emergjent prej 5 miliardë funte për të mbështetur NHS dhe shërbime të tjera publike në Angli; një e drejtë për pagë ligjore për të sëmurët, për individët që këshillohen të vet-izolohen; një ndihmë kontribuuese për mbështetjen e punësimit për punëtorët e vetëpunësuar; një fond për vështirësitë prej 500 milionë funte për këshillet për të ndihmuar më të prekshmit në zonat e tyre; një skemë kredie për ndërprerjen e punës së biznesit gjatë COVID19 për firmat e vogla dhe heqjen e normave të biznesit për kompani të caktuara. [45]

Ngjarje të tilla si këto rrisin gjasat e një përgjigje pozitive ndaj një fushate kriminale kibernetike dhe autorët e krimit ka shumë të ngjarë të lidhen me ngjarjet. Megjithëse duket se ekziston një lidhje midis disa prej ngjarjeve dhe incidenteve, një numër mashtrimesh nuk mund të gjurmohen lehtësisht në një ngjarje ose njoftim të vetëm. Shembuj të kësaj përfshijnë një pagesë të vullnetit të mirë prej 250 funte (21.03.2020), një kërkesë për dhurim financiar të NHS (02.04.2020), kupona për supermarkete të Mbretërisë së Bashkuar (02.04.2020, 15.04.2020, 28.04.2020), dhe një donacion bamirësie për pranuesin. Asnjë nga këto ngjarje nuk kanë shoqëruar njoftime qeveritare apo edhe spekulime të përgjithshme. [46]

2.3.5 Konkluzioni dhe puna në vazhdim

Pandemia COVID19 ka gjeneruar rrethana të jashtëzakonshme, unike shoqërore dhe ekonomike që mund të shfrytëzohen nga kriminelët kibernetikë. Analiza e ngjarjeve të tilla si njoftimet dhe historitë e mediave ka treguar atë që duket të jetë një ndërlidhje midis njoftimit dhe një fushate përkatëse të sulmit kibernetikë që përdor ngjarjen si një sulm duke rritur kështu gjasat e suksesit.

Pandemia COVID19 dhe shkalla e rritur e sulmeve kibernetike kanë shkaktuar pasoja më të mëdha, të cilat shtrihen përtej caqeve të sulmeve të tilla. Ndryshimet në praktikat e punës dhe shoqërisë do të thotë që njerëzit tani po kalojnë periudhë më të madhe të kohës në internet.

Përveç kësaj, nivelet e papunësisë janë rritur gjithashtu, që do të thotë që më shumë njerëz janë ulur në shtëpi në internet, ka të ngjarë që disa prej këtyre njerëzve t'i drejtohen krimit kibernetikë për të mbajtur veten. Kombinimi i niveleve të rritura të sulmeve kibernetike dhe krimit kibernetikë do të thotë se mund të ketë implikime për politikat rreth zbatimit të Ligjit Botëror në mënyrë që të sigurojë se ka aftësinë për të trajtuar krimin kibernetikë [47].

Analiza e paraqitur në këtë punim ka nxjerrë në pah një mjet të përbashkët të shumë sulmeve kibernetike gjatë kësaj periudhe. Shumë sulme kibernetike fillojnë me një fushatë mashtrimi e cila i drejton viktimat të shkarkojnë një skedar ose të hyjnë në një URL. Skedari ose URL-ja veprojnë si bartës të malware-it, i cili, kur instalohet, vepron si mjet për mashtrim financiar. Analiza ka treguar gjithashtu që për të rritur gjasat e suksesit, fushata e mashtrimit përdor media dhe njoftime qeveritare.

Edhe pse kjo analizë nuk është domosdoshmërisht e re, ne besojmë se është hera e parë që kjo mbështetet me një kontekst të ngjarjeve aktuale të drejtpërdrejta. Kjo analizë krijon rekomandimin që qeveritë, mediat dhe institucionet e tjera duhet të jenë të vetëdijshme se njoftimet dhe botimi i artikujve ka të ngjarë të shkaktojnë kryerjen e fushatave të sulmeve kibernetike që lidhen me këto ngjarje. Ngjarjet duhet të shoqërohen nga një shënim / mohim që përshkruan mënyrën e transmetimit të informacionit në lidhje me njoftimin.

Kërkimi ynë paraqet mundësi për hulumtime të mëtejshme. Ky hulumtim ka treguar atë që mund të përshkruhet më së miri si një korrelacion i lirshëm, i drejtpërdrejtë dhe i anasjelltë midis ngjarjeve dhe sulmeve kibernetike. Hulumtimet e mëtejshme duhet të hetojnë këtë fenomen dhe të përshkruajnë nëse një model parashikues mund të përdoret për të konfirmuar këtë marrëdhënie. Ekziston një furnizim i bollshëm i studimeve të rasteve të sulmeve kibernetike që lidhen me vendet në botë dhe një analizë më e gjerë e problemit mund të ndihmojë në afirmimin e këtij fenomeni.

3 DEKLARIMI I PROBLEMIT

Nga hulumtimet dhe shfletimi i literaturës, ne kemi zgjedhur temën të cilën do të trajtojmë, “Siguria kibernetike gjatë punës nga distanca” temë e cila ka shumë rëndësi të trajtohet, duke parë punën nga distanca si aktualitetin tonë të ri dhe nevojën esenciale për sigurinë kibernetike gjatë realizimit të punës nga distanca, në veçanti në këto kohë të pandemisë.

Gjatë hulumtimit ne kemi hasur në disa shembuj të punës nga distanca ku problemi i sigurisë kibernetike ishte një çështje e mbetur pa u trajtuar që prej fillesave të para të TI-së.

Të gjithë punonjësit dhe punëdhënësit nga distanca duhet të kenë parasysh sigurinë kibernetike ju nevojiten më shumë kujdes për këtë, pasi që jo çdo gjë është e mbrojtur pas mureve të organizatës.

Prandaj sot gjatë zbatimit të punës nga distanca duhet të kenë aftësi që të realizojnë punën nga distanca duke u kujdesur maksimalisht për rregullat dhe sigurinë kibernetike.

3.1 Pyetje Hulumtimi

Për të kuptuar më mirë çfarë duhet të kërkohet dhe analizohet në këtë temë, janë parashtruar tri pyetje hulumtimi.

1. Si ka ndikuar puna në distancë, në sigurinë kibernetike?
2. Çfarë praktika dhe hapa preventiv kanë ndjek kompanitë që të përgatitin për punëtoret të cilët do të punojnë nga distanca?
3. Cilat janë praktikat më të mira që kompanitë dhe individët duhet t’i ndjekin?

4 METODOLGJIA

Për hulumtime shkencore dhe prezantimin e rezultateve të tyre sa më mirë, përdoren shumë metoda shkencore. Gjatë punimit të temës, ne kemi përdorur disa metoda të ndryshme shkencore.

- Metoda historike të cilën e kemi përdorur për rishikimin e literaturës, duke analizuar literaturën dhe publikimet e ndryshme shkencore të cilat i referohen problemit të sigurisë kibernetike gjatë punës nga distanca.

- Metoda krahasuese, ku kemi marr shembujt më të njohur dhe aktual të sigurisë kibernetike dhe punës nga distanca.

- Metoda empirike është përdorur në pjesën më të madhe të kësaj teme, në të cilën ne kemi aplikuar përvojën e gjatë personale, në realizimin e punës nga distanca dhe rëndësinë e sigurisë kibernetike.

Rezultatet e prezantuara në këtë temë janë fituar si rezultat i një pune të gjatë, kronologjike, duke filluar me rishikimin e literaturës dhe analizën e gjendjes aktuale të sigurisë kibernetike gjatë punës nga distanca. Ndërsa, është marr modeli i Sulmit të Twitter, i cili sulm ndodhi gjatë punës nga distanca në kohën e pandemisë COVID19, ku në përfundim janë prezantuar përparësitë, mangësitë, sfidat dhe konkluzioni.

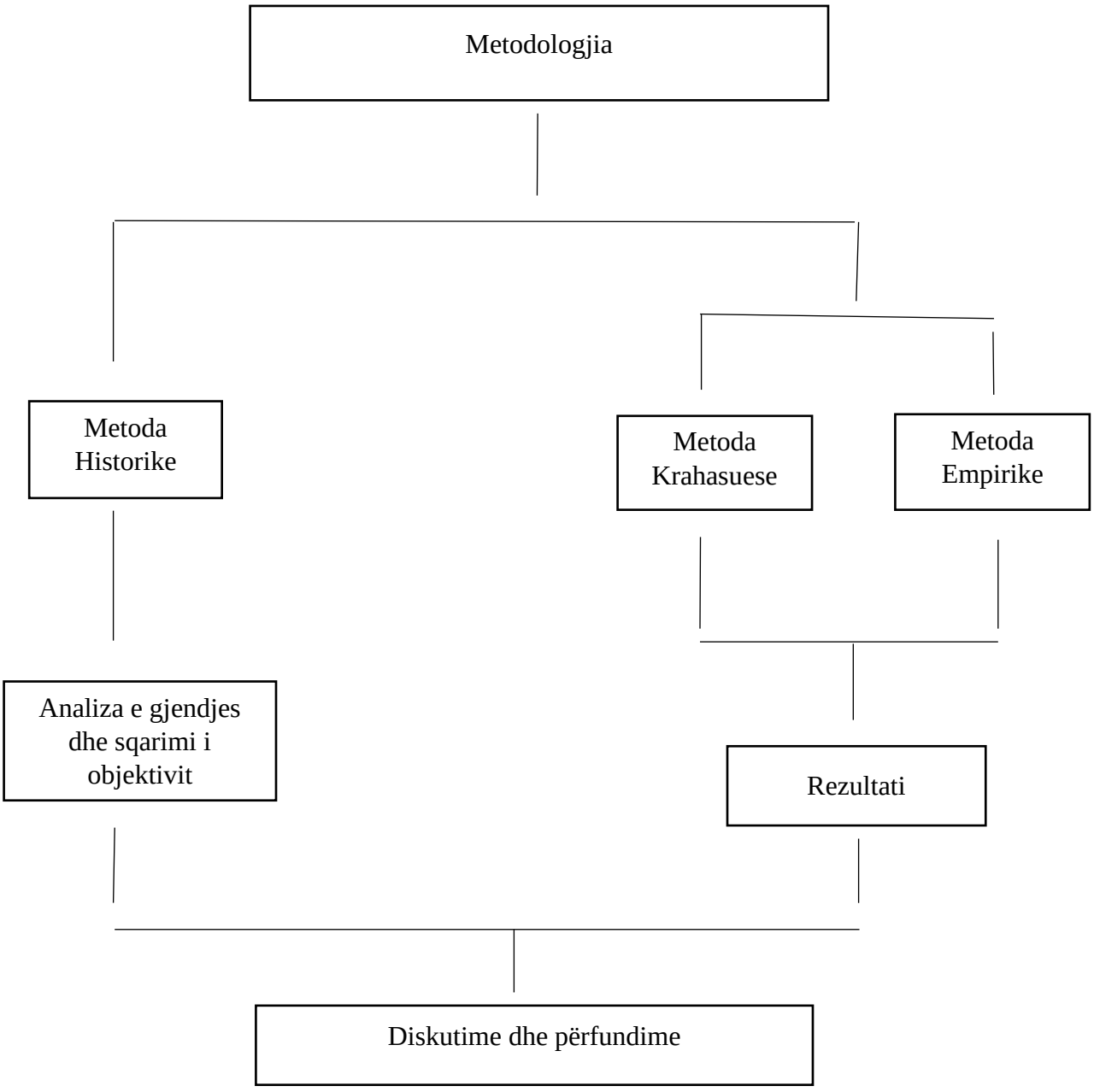

Figure 4. Metodologjia e përdorur për punimin e temës

5 REZULTATET – SHEMBUJ STUDIMI DHE KRAHASIMI QË E SHËNUAN VITIN 2020 PËR SIGURINË KIBERNETIKE GJATË PUNËS NGA DISTANCA

5.1 Sulmet kibernetike që e veçojnë vitin 2020 deri më tani

Viti 2020 është dalluar për shumë aspekte, ndër to është edhe rritja e sulmeve kibernetike. Një mundësi të jashtëzakonshme për sulmuesit kibernetikë për të hakuar dhe dëmtuar infrastrukturën TI-së së organizatave i dha edhe pandemia COVID19, sidomos organizimi i punës nga distanca.

Siguria e hapësirës në mes të rrjetit të shtëpisë dhe zyrës ka luajtur një rol kryesor për dëmtimin e të dhënave në vitin 2020. Kjo çështje ka rezultuar në vjedhje të informacionit konfidencial, duke çuar në humbjen e miliona dollarëve për organizatat e sulmuara.

Në fakt, 80% e firmave kanë parë një rritje të sulmeve kibernetike këtë vit. COVID19 ka një barrë të madhe të fajit për këtë rritje prej 238% të sulmeve kibernetike ndaj bankave. Sulmet phishing prej 600% që nga fundi i Shkurtit. [48]

Ndërsa, sulmet ransomware u rritën 148% në mars dhe pagesa mesatare e ransomware u rrit me 33% në 111,605 dollarë. [48]

Tabela 2. Rritja e sulmeve kibernetike në vitin 2020[4]

Lloji i sulmit	Rritja në përqindje në vitin 2020
Sulme kibernetike ndaj firmave	80%
Sulme kibernetike ndaj bankave	238%
Sulmet phishing	600%
Sulmet ransomware	148%

[4] Burimi: https://securityboulevard.com/2020/10/5-biggest-cyber-attacks-of-2020-so-far/

Duke qenë se po flasim për një rritje dramatike të sulmeve kibernetike, në vazhdim do të paraqesim pesë sulmet e mëdha kibernetike që kanë ndodhur në vitin 2020 deri më tani, të cilat kanë dëmtuar disa organizata të famshme botërore.

5.1.1 Sulmi ransomware ndaj Software AG

Shitësi i njohur gjerman i softuerëve, Software AG, është goditur nga një sulm ransomware në tetor të vitit 2020. Firma gjermane e teknologjisë është sulmuar nga ransomware Clop dhe banda kriminale kibernetike ka kërkuar më shumë se 20 milionë dollarë shpërblim.

Raporti gjithashtu thotë se kompania ende nuk është rikuperuar plotësisht nga sulmi. Kompania zbuloi se sulmi ransomware prishi një pjesë të rrjetit të saj të brendshëm. Por shërbimet për klientët e saj, përfshirë shërbimet e bazuara në cloud, mbetën të paprekura. Kompania gjithashtu u përpoq të negocionte me sulmuesit, por gjithçka shkoi kot.

Sipas deklaratës së lëshuar nga Software AG, kompania është në proces të rivendosjes së sistemit dhe bazës së të dhënave për të rifilluar funksionimin e rregullt. [48]

5.1.2 Sulmi ransomware ndaj Sopra Steria

Gjigandi francez i shërbimeve të TI-së Sopra Steria u sulmua nga ransomware në mbrëmjen e 20 tetorit 2020, siç konfirmohet nga kompania. Biznesi i tij i teknologjisë financiare, Sopra Banking Software, identifikoi virusin që është një version i ri i ransomware Ryuk, i cili ishte i panjohur më parë për ofruesit e sigurisë kibernetike.

Sopra Steria pretendoi se ishte në gjendje ta kufizonte sulmin në një pjesë të kufizuar të sistemit të saj të TI-së, edhe pse e kapi sulmin pas disa ditësh. Sidoqoftë, pas një hetimi të thelluar, kompania nuk identifikoi ndonjë dëmtim ose rrjedhje të të dhënave që i ishte shkaktuar ndaj klientëve të saj.

Ryuk është një nga ransomware-ët më inovativ që tashmë ka targetuar organizata EWA, organizatë e kontraktuar nga departamenti amerikan i mbrojtjes dhe Prosegur, një firmë logjistike Spanjolle. [48]

5.1.3 Rrëmbimi i Telegramit

Në shtator të vitit 2020, hakerat fituan qasjen në aplikacionin Telegram të mesazheve dhe të dhënat e postës elektronike të disa emrave të mëdhenj në biznesin e kriptomonedhave. Hakerat përdorën Sistemin e Sinjalizimit 7 (SS7), i cili përdoret për lidhjen e rrjeteve celulare në të gjithë botën, për të hakuar të dhënat.

Sipas ekspertëve të sigurisë kibernetike, hakerat ishin vënë pas kodeve të identifikimit me dy faktorë (2FA). Ata mashtruan qendrën e shërbimit të mesazheve të shkurtra (SMSC) të operatorëve të rrjetit celular për të dërguar një kërkesë për azhurnimet e vendndodhjeve të paktën 20 viktimave të profilit të lartë.

Ky sulm besohet të ketë ndodhur për të marrë kriptovaluta. Ky lloj sulmi kibernetik është i njohur mirë në komunitetin e kriptomonedhave dhe përdoruesit në përgjithësi janë të vetëdijshëm për kërkesa të tilla.

Prandaj, në komunitetin e kriptomonedhave ekzistojnë metoda më të mira të vërtetimit sesa thjesht SMS ose 2FA e bazuar në thirrje. Ekspertët e sigurisë kibernetike mendojnë se standardet e telekomit të cilat nuk mund të zgjidhin çështje moderne, duhet të largohen nga përdorimi i protokolleve si SS7. [48]

5.1.4 Sulmi ndaj Seyfarth Shaw Malware

Firma ligjore, lidere në tregun ndërkombëtar, me bazë në Çikago, Seyfarth Shaw LLP u bë viktimë e një sulmi agresiv keqdashës "malware agresive". Ky sulm u konfirmua më vonë nga firma si një sulm ransomware. Sulmi kibernetik thuhet se ndodhi më 10 tetor 2020 dhe rrëzoi plotësisht sistemin e postës elektronike të firmës, sipas një deklarate të botuar nga kompania.

Firma pretendoi në deklaratën e saj se nuk kishte asnjë provë të të dhënave të klientit ose të të dhënave të firmës, hyrje ose largim i paautorizuar. Sidoqoftë, shumë nga sistemet e saj u gjetën të koduara, që pas kësaj firma i mbylli të gjitha, si një masë parandaluese.

Firma ligjore njoftoi FBI-në si organ kompetent për zbatimin e ligjit, e cila tashmë ka filluar hetimet. Përveç kësaj, asnjë informacion i mëtejshëm nuk na zbuloi se si ndodhi sulmi dhe çfarë familje e ransomware-ëve goditi firmën. [48]

5.1.5 Shkelja e sigurisë së të dhënave të korporatës Carnival Corporation

Operatori më i madh i linjës së anijeve turistike në botë, Carnival Corporation raportoi një shkelje të të dhënave për shkak të një sulmi ransomware që ndodhi në muajin Gusht 2020. Hakerat vodhën informacione konfidenciale të klientëve, punonjësve dhe anëtarëve të ekuipazhit gjatë kohës së sulmit.

Më 15 gusht, 2020, kompania zbuloi sulmin ransomware që dëmtoi dhe kriptoi një nga infrastrukturat TI-së të markës së saj. Pas sulmit, operatori i linjës së anijeve turistike njoftoi organet kompetente për zbatimin e ligjit dhe punësoi këshilltarë ligjorë dhe ekspertë të sigurisë kibernetike dhe filloi një hetim.

Megjithëse kompania pretendoi se asnjë keqpërdorim i të dhënave personale të ekspozuara nuk ka dalë në dritë, lloji i ransomware-it dhe mënyra se si ndodhi sulmi kanë mbetur të pazbuluara. [48]

Tabela 3. Arsyeja e rritjes së sulmeve[5]

Arsyet e sulmeve	Përqindja
Sulmet ndaj llogarive	67%
Rritja e ransomware	27%
Dobësitë e web- aplikacioneve	43%
Sulmet ndaj të dhënave personale	58%
Shkeljet nga gabimet vazhdojnë të jenë problem	17%

5.2 Thyerja më e madhe e sigurisë në Twitter: Llogaritë e profileve të larta amerikane të hackuara në mashtrimin me Bitcoin

Më 15 korrik 2020, rreth orës 04:00 pasdite në SHBA, shumë llogari të personaliteteve të profilit të lartë në Twitter duke përfshirë Barack Obama, Elon Musk, Bill Gates, Jeff Bezos u hakuan.

[5] Burimi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950063/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised_V2.pdf

Mesazhi në Twitter tha se çdo bitcoin i dërguar në linkun e bashkangjitur në cicërimë do të kthehej i dyfishuar.

Cicërimat e rreme ofronin 2,000 dollarë për çdo 1,000 dollarë të dërguara në një adresë të Bitcoin. Mashtruesit më vonë fshinë cicërimat dhe ndanë përsëri ato duke kërkuar të njëjtën gjë. Në përgjigje të incidentit, ekipi i mbështetjes së Twitter menjëherë bllokoi aktivitetet e llogarive të prekura. [49]

Edhe pse Twitter u përpoq të rimarrë kontrollin duke fshirë këto cicërima, disa nga keqpërdoruesit e llogarive filluan të postonin përsëri të njëjtat mesazhe. Sulmi konsiderohet të jetë njëri nga sulmet kibernetike mbi media sociale më i madh i gjitha kohërave dhe si sulmi më i pacipë në historinë e internetit!

Llogaritë në Twitter të politikanëve të mëdhenj amerikanë, të famshmëve dhe personaliteteve të profilit të lartë u hakuan. Emrat e përdoruesve të verifikuar ishin ndër të tjerë, ish presidenti i SHBA-së Barack Obama, Joe Biden, Apple, Uber, Elon Musk, Kanye West, Bill Gates, Kim Kardashian.

Ndërsa cicërimet u bënë virale, shumë përdorues të Twitter-it e përqeshën atë duke e krahasuar me “Money Heist”. Sidoqoftë, disa përdorues i konstatuan si të vërteta dhe ligjore këto cicërima dhe dhanë bitcoin-ët e tyre. Rreth mijëra njerëz u mashtruan pasi ranë viktima të llogarive të kompromet uara që premtuan të dyfishojnë shumën e dërguar nga adhuruesit e tyre përmes kriptovalutës Bitcoin. [49]

Raportohet se në këtë mashtrim të koordinuar mirë, mesazhet nga kriminelët kibernetikë arritën të paktën 350 milionë përdorues me ndihmën e sistemeve të brendshme të Twitter. Mashtruesit mbrapa kësaj shkelje masive përfituan 120,000 dollarë vlerë në bitcoin përmes të paktën 300 transaksioneve. [49]

Sidoqoftë, Komiteti i Tregtisë i Senatit të SHBA-së ka kërkuar një përmbledhje të shkurtër mbi incidentin nga Twitter-i. Sipas gjigantit të mediave sociale, ishte një sulm "i koordinuar" që ka targetuar punonjësit e Twitter me qasje në mjetet dhe sistemet e brendshme. [49]

5.2.1 Si ndodhi Hakimi?

Një punonjës nga Twitter thuhet se ishte arsyeja prapa hakimit të koordinuar të Twitter-it, por hetimi po vazhdon ende. Sipas burimit, një nga hakerat deklaroi se ata përdorën një përfaqësues që bëri të gjithë punën për hakerat në sulm. Një tjetër deklaroi se ata paguan një person të brendshëm.

Është raportuar se një mjet i brendshëm u përdor në këtë sulm për të rivendosur adresat e lidhura të postës elektronike të llogarive të hakuara, për ta bërë më të vështirë për pronarët e llogarive që të rimarrin kontrollin. Pastaj, ata shtyn një mashtrim kriptovalutash dhe filluan të gjithë sulmin. [49]

5.2.2 Si mbijetoi Twitter hakimin e tij më të madh - dhe planet për të ndaluar tjetrin

15 Korriku në fillim ishte një ditë e zakonshme për Parag Agrawal, shefi i teknologjisë së Twitter. Agrawal u vendos në zyrën e tij të shtëpisë në Bay Area, në një dhomë që ai ndan me djalin e tij të vogël. Ai filloi të punonte detyrat e tij të rregullta - integrimin e të mësuarit thellë në algoritmet thelbësore të Twitter, duke mbajtur gjithçka nën kontroll dhe duke kundërshtuar rrjedhat e vazhdueshme të keqinformimit, dezinformimit dhe keqinformimit në platformë. [50]

Por nga mesi i mëngjesit në Bregun Perëndimor, sinjalet e shqetësimit kishin filluar të shfaqeshin nëpër organizatë. Dikush po përpiqej të merrte kredencialet e punonjësve dhe ata po bënin punë shumë të mirë. Ata po thërrisnin personelin e shërbimit të konsumatorit dhe mbështetjen e teknologjisë, duke i udhëzuar ata të ripërtërinin fjalëkalimet e tyre. Shumë punonjës i kaluan mesazhet ekipit të sigurisë dhe u kthyen në punë. Por disa të pakujdesshëm - mbase katër, ndoshta gjashtë, ndoshta tetë - ishin më lehtë për t'u mashtruar. Ata shkuan në një faqe të kontrolluar nga hakerat dhe futën kredencialet e tyre në një mënyrë që i udhëzonte të shkruajnë emrat dhe fjalëkalimet e tyre, si dhe kodet e vërtetimit shumë faktorësh. [50]

Pas pak, disa llogari në Twitter me adresa të profilit të shkurtra: @drug, @xx, @ vampire dhe më shumë, u kompromet uan. Të ashtuquajturit emra përdoruesish autentik vlerësohen midis bashkësive të hakerëve, në mënyrën se si vlerësohen veprat e artit impresionistë në Anën e Sipërme Lindore. Twitter e di këtë dhe i shikon ata me prioritet të lartë. Por, problemi nuk shkoi deri tek Agrawal. Twitter ka një ekip të dedikuar për "Zbulim dhe Përgjigje" që shtjellon incidentet e

sigurisë. DART kishte zbuluar një aktivitet të dyshimtë, por përgjigjja e nevojshme ishte e kufizuar, këto lloj gjërash ndodhin gjatë gjithë kohës. [50]

Por më pas, në orën 3:13 pasdite, me orën lindore, platforma e shkëmbimit të kriptovalutave Binance dërgoi një cicërimë të pazakontë duke njoftuar se po "dhuronte" rreth 52 milionë dollarë Bitcoin për komunitetin përmes një linku të një ueb-faqeje mashtruese. Për gjatë orës tjetër, 11 llogari të kriptomonedhave ndoqën shembullin. Dhe më pas, në 4:17 pasdite ET, @elonmusk shkroi në Twitter një mashtrim klasik për gati 40 milionë ndjekësit e tij. Disa minuta më vonë, @billgates bëri të njëjtën gjë. [50]

Së shpejti, çdo pajisje njoftimi që kishte Agrawal po gumëzhinte: Slack, email, mesazhet, gjithçka. Diçka po shkonte tmerrësisht keq. Në 4:55 pasdite ET cicërimat erdhën më shpejtësi: Uber, Apple, Kanye West. Jeff Bezos, Mike Bloomberg dhe Elon Musk, përsëri. Twitter ishte duke u sulmuar.

Në ato momente kishte shumë ndenja, por ajo kryesore ishte pasiguria dhe frika pasi që llogari të profilit të lartë po sulmoheshin. Sistemi ishte kompromentuar dhe Twitter duhet të vendoste si të vepronte në vazhdim. Të mbyllen të gjitha llogaritë? Të mbyllin vetëm disa? Të gjithë në kompani ndiheshin sikur kishin nevojë të përgjigjeshin, por askush nuk ishte saktësisht i sigurt se si. "Ishte një rrezik i pakufizuar", thotë Agrawal.

Ai moment tronditës dhe ajo ditë tronditëse, ngritën gjithashtu një perspektivë edhe më hidhëruese: Po sikur dikush të hakonte platformën për të përmbysur demokracinë amerikane? Që nga ai moment, kompania ka filluar një përpjekje për të forcuar mbrojtjen e saj para 3 nëntorit dhe ajo ka filluar ndryshimet për të mbrojtur më mirë sistemet e saj, përdoruesit e saj dhe vetë demokracinë amerikane. Sot, në fakt, ajo po njofton një seri të protokolleve të reja të sigurisë, trajnimeve të detyrueshme të punonjësve dhe ndërrimeve të politikave. Për të kuptuar pse, është e rëndësishme të kthehemi në 15 korrik dhe kaosin që përfshiu Twitter.

Orët që pasuan cicërimet e bitcoin ishin disa nga më kaotiket në historinë e Twitter, si në platformë ashtu edhe brenda kompanisë.

Në mënyrë ideale, sistemet e automatizuara do të kishin identifikuar se cilët përfaqësues të Twitter po ndryshonin të gjitha ato adresa email-i në një kohë kaq të shkurtër. Por një ish-punonjës i sigurisë në Twitter thotë se kompania kishte qenë e ngadaltë për të investuar në atë lloj teknologjie

të paralajmërimit të hershëm dhe se një kulturë besimi e kishte zbehur atë ndaj kërcënimeve të mundshme, të brendshme. [50]

Për shkak se nuk dihej nga vinte sulmi, Twitter nuk mund të parashikonte se cili person i famshëm mund të hakohej në vijim. Çaktivizimi i shërbimit fare nuk ishte praktik; sipas një ish-ekzekutivi, nuk është as e qartë nëse Twitter mund ta bënte një gjë të tillë lehtë, nëse do të duhej. Por deri në orën 6:18 pasdite ET ekipi vendosi për gjënë më të ashpër: Bllokoni të gjitha llogaritë e verifikuara nga cicërimat. Ata vendosën kufizime të mëtejshme në çdo llogari që kishte ndryshuar fjalëkalimin e tyre në javët e kaluara. [50]

Kaosi pasoi, me shumë prej atyre që ende mund të cicëronin duke festuar heshtjen e "verifikimeve blu". Por gjithashtu krijoi një ngushtim informacioni. Shërbimi Kombëtar i Motit nuk mund të dërgonte një këshillues për tornado dhe kompanitë e medias, duke përfshirë WIRED, nuk ishin në gjendje të cicërojnë lajme në lidhje me hakimin, duke lënë llogarinë zyrtare të Mbështetjes së Twitter si burimin kryesor të besueshëm të informacionit në platformë. Përditësimet shpërthyen për një temë të gjatë që përfundimisht do të shtrihej deri në shtator, me Twitter duke ndarë atë që dinte në thelb në kohë reale. Dhe ajo që dinte ishte kjo: Të paktën një nga ato telefonatat phishing kishte funksionuar.

Brenda Twitter-it, Agrawal dhe ekipi i tij punuan furishëm përmes shkëmbimeve të njohurive të tyre të mundshme të veprimit. Sa më fort të mbyllni rrjetin e brendshëm, aq më pak jeni në gjendje t'i kundërviheni mashtrimit. Ju gjithashtu humbni aftësinë për të gjetur autorët ose për të kuptuar se kush në ekipin tuaj është kompromentuar. Kështu që ata vendosën një hap të parë të moderuar: Ata do të përjashtonin të gjithë nga VPN-i i brendshëm. Ata nuk donin t'i bënin të gjitha menjëherë sepse nuk donin që ekipi i përgjigjes së sigurisë të humbasë qasjen, ose të mbingarkojnë potencialisht sistemin ndërsa të gjithë nxitonin të qaseshin përsëri. Ata ndërprenë hyrjen në një qendër të të dhënave në të njëjtën kohë.

Më pas ata filluan procesin e detyrimit të punonjësve të hynin në mjedisin e “zero besimit” ashtu siç e quanin profesionistët e sigurisë. Duke filluar me CEO Jack Dorsey dhe më pas me punonjësit e tjerë, çdo person duhej të hynte në një video konferencë me mbikëqyrësin e tyre dhe të ndryshonte fjalëkalimet e tyre para tyre. Ishte versioni i epokës COVID që kërkonte nga të gjithë të hynin në një linjë jashtë tryezës së TI-së. Agrawal shpejt ishte në një takim me të gjithë ekipin

ekzekutiv, jo për të planifikuar përgjigjen, por për të konfirmuar që të gjithë ishin ata që thanë se ishin.

Një ish-punonjës i lartë i Twitter thotë: “Pati një dështim të nivelit të sistemeve. E gjithë kjo gjë nuk duhet të kishte ndodhur. Çështja nuk është se dikush u mashtrua, është se sapo ata u mashtruan, kompania duhet të kishte sistemet e duhura për t'u përballur me të ".

Twitter është përballur më parë me marrjen e llogarive. Vetë Jack Dorsey humbi kontrollin e llogarisë e tij më shumë se një vit më parë. Sidoqoftë, ato incidente kanë ardhur kryesisht nga dobësitë në aplikacionet e palëve të treta ose, në rastin e Dorsey, nga të ashtuquajturat sulme SIM-swap që transferojnë numrin e telefonit të dikujt në pajisjen e një hakeri. Hakimi i 15 korrikut ishte e ndryshme sepse ndikoi në vetë sistemet e Twitter. Dhe për shkak se organizatori i tij i pretenduar ishte një adoleshent në Florida.

Sipas akuzave të ngritura nga Departamenti i Drejtësisë dhe Zyra e Prokurorit të Shtetit të Hillsborough County, skema u orkestrua nga Graham Ivan Clark, një 17-vjeçar nga Tampa, Florida, i cili më parë ishte specializuar në mashtrimin e njerëzve në Minecraft. Clark ishte pjesë e komunitetit të ndërrimit të kartave SIM, i cili zakonisht është përqendruar në vjedhjen e kriptovalutave. Por Clark ishte gjithashtu i njohur me OGUsers, një komunitet në internet që fiksohet pas emrave të përdoruesve të shkurtër dhe të zakonshëm. Ndërsa sulmi në Twitter do të përfundonte me 130 llogari në shënjestër, shënjestra dyshohet se filloi me shumë më pak. Ai dyshohet se e kreu sulmin me partnerin Nima Fazeli. Me ndihmën e Fazeli dhe një ndërmjetësi tjetër, Clark dyshohet se ka marrë mijëra dollarë për qasje të drejtpërdrejtë në llogari. Ai shpejt kishte aspiruar nga mashtrimi i adoleshentëve në Minecraft tek kontrollimi i llogarive të njerëzve me vlerë rreth një trilion dollarë.

5.2.3 Si u kapën hakerat e supozuar të Twitter-it

Sipas prokurorëve, Clark atë ditë përmirësoj planin e tij fillestar: marrja përsipër e @kanyewest është më interesante sesa marrja e @SC. Së shpejti ai dyshohet se mori ato të Musk, Gates, Jeff Bezos, Joe Biden dhe të tjerëve, duke mbledhur rreth 117,000 dollarë në mashtrimin e tij rudimentar me bitcoin. Clark u deklarua i pafajshëm për 30 akuza në 4 Gusht. Agjentët federalë thuhet se po hetojnë gjithashtu një adoleshent të Massachusetts në lidhje me sulmin.

Twitter duket se nuk ka gjasa të bjerë përsëri viktimë e këtij sulmi të njëjtë, të paktën jo së shpejti. Përdoruesit e OGUsers janë duke qëndruar jo aktiv për momentin, thotë Allison Nixon, zyrtari kryesor i kërkimit të firmës së sigurisë Unit 221B, i cili ndihmoi FBI-në në hetimin e saj. Por kjo nuk do të thotë që kompania mund të mbetet e qetë. "Me sa duket sulmi prishi këtë metodë", thotë Nixon. "Sa i përket zgjedhjeve, do të ketë kaq shumë kaos dhe do të jetë problem të kontrollohen." Nëse një adoleshent me qasje mundet ta sjell kompaninë në gjunjë, ta imagjinojmë se çfarë mund të bëjë Vladimir Putin.

U desh rreth një muaj që Twitter të rikthehej sadopak normal, pasi punonjësit rifituan mjetet që në përgjigjen fillestare u ishin mohuar, por jo të gjithë dhe jo në çdo kohë. Nëse do të drejtoni një kompani të mediave sociale, duhet të keni disa njerëz me qasje në disa llogari. Lady Gaga mund ta harrojë fjalëkalimin e saj. Elon Musk mund të humbasë telefonin e tij. Dikush mund të shkelë kushtet e shërbimit të kompanisë dhe duhet të ndalohet, që do të thotë se dikush duhet të jetë në gjendje t'i ndalojë ata. Siç theksojnë drejtuesit në kompani, të bësh mirë nga përdoruesit e tu mund të bie ndesh me mbajtjen e platformës së sigurt.

Por një nga gjërat e para që Twitter kuptoj menjëherë pas kësaj ishte se shumë njerëz kishin shumë qasje në shumë gjëra. "Është më shumë se sa keni besim tek secili person dhe sa personave ju besoni në përgjithësi", thotë Agrawal. "Sasia e qasjes, sasia e besimit të dhënë për personat me qasje në këto mjete, është dukshëm më e ulët sot."

Një nga ndryshimet më të mëdha që kompania ka zbatuar është që t'u kërkojë të gjithë punonjësve të përdorin vërtetimin fizik me dy faktorë. Twitter tashmë kishte filluar shpërndarjen e çelësave të sigurisë fizike për punonjësit e saj përpara hakimit, por tani rriti përhapjen e programit. Brenda disa javësh, të gjithë në Twitter, përfshirë kontraktorët, do të kenë një çelës sigurie dhe do të kërkohet ta përdorin atë. Ky ndryshim përshtatet mirë në një kornizë që Stamos sugjeroi. Ekzistojnë kryesisht tre mënyra si mund të vërtetosh dikë: me emrin e përdoruesit dhe fjalëkalimin e tij, me vërtetimin me dy faktorë dhe me një pajisje të dhuruar nga kompania që mund ta gjurmosh. "Për shumicën e gjërave, duhet të keni dy prej tyre", thotë ai. "Për gjëra kritike, duhet t'i keni të tria."

Aspekti më bezdisës i hakimit në Twitter është te fakti se sa më keq mund të ketë qenë. Hetimi i Twitter zbuloi që sulmuesit kishin hyrë në mesazhet direkte të 36 prej 130 targeteve. Ata shkarkuan informacionin "Të dhënat e tua në Twitter" për tetë viktima, që përfshijnë çdo cicërimë që ata kanë

dërguar - përfshirë mesazhe private direkte - kur dhe ku ishin në atë kohë, dhe në cilat pajisje përdorin Twitter-in. Një haker më i interesuar në spiunazh sesa në kripto-monedha do të donte të kishte atë lloj qasje.

Megjithatë, 15 korriku tregon se jo çdo krizë mund të provohet. Një mënyrë për të kapërcyer kufijtë e imagjinatës është të bëni ndryshime strukturore. Përveç çelësave të vërtetimit fizik që punonjësit e Twitter së shpejti filluan të përdorin, kompania ka forcuar regjimin e saj të trajnimit të brendshëm. Të gjithë punonjësit do t'i nënshtrohen kontrolleve të zgjeruara dhe të gjithëve tani u kërkohet të përfundojnë kurse për të kuptuar privatësinë dhe për të shmangur mashtrimin. Nuk është e qartë se çfarë ndodhi me punonjësit që u mashtruan në korrik. Për të mbrojtur privatësinë e tyre dhe për shkak të hetimit të vazhdueshëm të DOJ, kompania nuk do të tregoj kush janë ata. Deri më sot vetëm një pjesë e vogël e njerëzve në Twitter e dinë. [50]

Kompania tani po tregohet më largpamëse, duke vendosur kërkesa më të rrepta për fjalëkalimin te përdoruesit në rrezik si politikanët, llogaritë e fushatave dhe gazetarët politikë. Inkurajon, por nuk urdhëron ato llogari për të vënë në funksion vërtetimin me dy faktorë. Gjithashtu mbetet e paqartë shkalla në të cilën Twitter po ndërton masa shtesë mbrojtëse të brendshme dhe për cilat llogari. [50]

5.2.4 Mësimet e sigurisë kibernetike nga Hakimi i Twitter të nxjerra nga Rregullatori i Shërbimeve Financiare të New York-ut

Ka mësime të sigurisë kibernetike që duhet të mësohen nga shkeljet e të dhënave të profilit të lartë dhe si kundërpërgjigje pasojnë rregulloret. Reklamë e publikuar mirë për vetëdijesimin ndaj sigurisë kibernetike ka qenë edhe hakimi i Twitter. Sipas hetimit dhe raportit të Departamentit të Shtetit të Shërbimeve Financiare të New York-ut ("NYSDFS"), për “Hakimin e Twitter”. NYSDFS arriti në përfundimin se masat mbrojtëse të sigurisë kibernetike të Twitter ishin të papërshtatshme, duke lejuar hakerët të imitojnë politikanë, njerëz të famshëm, sipërmarrës dhe disa kompani kripto-valutash duke abuzuar me llogaritë e tyre në Twitter për të kërkuar pagesa bitcoin në një mashtrim "dyfisho bitcoin-in tuaj". Rezultatet kryesore ishin që mediat sociale dhe organizatat e konsumatorëve duhet të zhvillojnë trajnime gjithëpërfshirëse të të gjithë punëtorëve lidhur me sigurinë kibernetike, të kenë një menaxhment të përgatitur të sigurisë kibernetike që menaxhon në mënyrë efektive hyrjen dhe vërtetimin e llogarisë dhe gjithashtu të përdorin një

zgjidhje të Menaxhimit të Ngjarjeve të Sigurisë (SIEM) për të zbuluar dhe përgjigjur kërcënimeve në kohë reale. Veçanërisht, në dritën e gjetjeve të saj, NYSDFS tani po bën thirrje për rregullimin e përkushtuar të sigurisë kibernetike të kompanive të mëdha të mediave sociale, e ngjashme me rregulloren e sigurisë kibernetike NYSDFS për organizatat e shërbimeve financiare sepse " rreziku që paraqesin mediat sociale për konsumatorët tanë, ekonominë, dhe demokracinë nuk është më pak i rëndë se rreziqet që paraqesin institucionet e mëdha financiare. ” [51]

NYSDFS përfundoi: “Hakimi i Twitter është një tregim paralajmërues për dëmin e jashtëzakonshëm që mund të shkaktohet edhe nga kriminelë jo të sofistikuar kibernetikë. Suksesi i hakerëve ishte kryesisht për shkak të dobësive në protokollet e brendshme të sigurisë kibernetike të Twitter. ” NYSDFS zbuloi se Twitter nuk kishte asnjë zyrtar kryesor të sigurisë së informacionit që nga dhjetori 2019, që prej shtatë muaj para sulmit në Twitter. Raporti gjithashtu zbuloi se hakerët shfrytëzuan drejtpërdrejt kalimin e Twitter me punë nga distanca gjatë pandemisë. Sipas NYSDFS: “Niveli i punës nga largësia në Mars 2020 vendosi një tendosje në infrastrukturën e teknologjisë së Twitter dhe punonjësit kishin probleme të shpeshta me lidhjet VPN në rrjet. Hakerët përfituan nga këto çështje dhe pretenduan se po telefononin nga departamenti i TI-së në Twitter për një problem të VPN. ” Hakerat kishin hulumtuar organizatën e Twitter duke mësuar funksionet themelore dhe titujt e punonjësve të Twitter, kështu që ata mund të imitonin në mënyrë më efektive departamentin e TI-së së Twitter. Pavarësisht udhëzimeve publike nga autoritete të shumta rregullatore, duke përfshirë NYSDFS, për të identifikuar dhe për t'iu përgjigjur rreziqeve të sigurisë kibernetike gjatë pandemisë, NYSDFS zbuloi se Twitter nuk zbatoi ndonjë kontroll domethënës kompenzues pas Marsit 2020 për të zbutur këtë rrezik të rritur me realizimin e punës nga distanca, hakerët e morën si avantazh dhe u përpoqën të kryenin mashtrime financiare të shumëllojshme. [51]

NYSDFS arriti në përfundimin se megjithëse Twitter i nënshtrohet ligjeve të zbatueshme për privatësinë e të dhënave dhe sigurinë kibernetike, të tilla si Akti i Privatësisë së Konsumatorit në Kaliforni, Akti i New York SHIELD dhe Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave të Bashkimit Evropian, pavarësisht se të gjitha rregullojnë ruajtjen dhe përdorimin e të dhënave, nuk ka rregullore që ka autoritetin për të rregulluar në mënyrë uniforme platformat e mediave sociale që veprojnë në internet dhe për të adresuar shqetësimet e sigurisë kibernetike të identifikuara në këtë raport. Ky vakum i rregulloreve duhet të plotësohet. [51]

Ndërsa mbetet për t'u parë nëse raporti i NYSDFS përfundimisht do të ndikojë në hartimin e një rregulloreje të re kombëtare të sigurisë kibernetike, mediat sociale dhe organizatat e tjera që përballen me konsumatorët duhet të shohin praktikat e tyre duke u bazuar në shembullin e harkimit të Twitter dhe të marrin hapa tani për të adresuar rreziqet e punëtorëve nga distanca.

6 DISKUTIME DHE PËRFUNDIME

Kjo temë është trajtuar si rezultat i një analize për këtë problem si mjaft aktual ditëve të sotme. Është rishikuar shumë literaturë dhe janë shpjeguar nocionet dhe historia e sigurisë kibernetike dhe punës nga distanca. Në të njëjtën kohë është realizuar hulumtimi dhe analiza e gjendjes aktuale të sigurisë kibernetike gjatë punës nga distanca, në kohën e pandemisë COVID19. Të gjitha të dhënat që kemi mbledhur nga statistikat e paraqitura në media dhe faqe të ndryshme zyrtare. Janë identifikuar shumë shembuj të sulmeve kibernetike të vitit të fundit. Si shembull kryesor është marr rasti i "Hakimit të rrjetit social Twitter" si rast që ka filluar të ndikoj në rishikimin e rregulloreve për sigurinë e mediave sociale.

Pas realizimit të gjithë kësaj pune janë ofruar konkluzionet dhe rekomandimet bazuar në pyetjet e zgjedhura gjatë deklarimit të problemit. Ne kemi ardhur në përfundim se këto konkluzione dhe rekomandime do të ndihmonin në sigurinë kibernetike të çdo organizate.

1. Si ka ndikuar puna në distancë, në sigurinë kibernetike?

Tranzicioni global në kulturën e punës nga shtëpia ka krijuar një mënyrë që kryesit e krimeve kibernetike të ekzekutojnë sulme kibernetike tepër të përparuara. Për më tepër, ransomware, phishing, DDoS, malware, etj., janë ndër format më të spikatura të sulmeve kibernetike që kemi provuar këtë vit, deri më tani.

2. Çfarë praktika dhe hapa preventiv kanë ndjek kompanitë që të përgatitin për punëtorët të cilët do të punojnë nga distanca?

   Në vazhdim kemi hartuar një listë të masave që "duhet të ndjeken" për të siguruar organizatën kundër sulmeve të reja kibernetike:

   1. Kryeni VAPT (Vlerësimin e Cenueshmërisë dhe Testet e Depërtueshmërisë - Penetrimit) për të kontrolluar në mënyrë periodike dobësitë e sigurisë që mund të shfrytëzohen në infrastrukturën e TI-së së organizatës suaj.

2. Krijoni një kopje rezervë të të gjitha të dhënave të ndjeshme ose konfidenciale dhe ruani ato ndaras nga njëra tjetra herë pas here.

3. Mbani të gjitha sistemet, softuerin dhe aplikacionet të azhurnuara me përditësimet më të fundit të sigurisë.

4. Kufizoni punonjësit nga ndarja e fjalëkalimeve në punë dhe inkurajoni ata të përdorin fjalëkalime unike dhe të forta.

5. Bllokoni mashtrimet e postës elektronike, postën e bezdisshme dhe sulmin BEC duke siguruar domenin tuaj të postës elektronike me protokollet e vërtetimit të postës elektronike si DMARC, SPF dhe DKIM.

6. Drejtoni një fushatë simulimi të sulmeve kibernetike për të vlerësuar nivelin e ndërgjegjësimit kibernetikë midis punonjësve. Pastaj trajnoni në përputhje me rrethanat, me mjetin më të mirë për trajnimin e vetëdijesimit për sigurinë.

7. Sigurohuni që të zbatoni praktikën e përdorimit të vërtetimit me shumë faktorë për të ruajtur sigurinë dhe privatësinë.

8. Kufizoni administratorin e TI-së dhe të drejtat e qasjes për punonjësit me të drejta të kufizuara. Sigurohuni që ata të jenë të trajnuar në mënyrë adekuate për përdorimin e sigurt dhe ruajtjen e koduar të të dhënave të ndjeshme.

3. Cilat janë praktikat më të mira që kompanitë dhe individët duhet t’i ndjekin

Incidentet e fundit kanë nxjerrë në pah nevojën urgjente për të gjitha platformat e mediave sociale dhe kompanitë e tjera, për të kontrolluar masat e tyre të sigurisë. Lidhja më e dobët në zinxhirin e sigurisë kibernetike është “përdoruesi”.

Pavarësisht se sa programe sigurie të vendosura në fund të fundit, organizatat duhet t'u ofrojnë punonjësve të tyre trajnimin e duhur për vetëdijesimin mbi sigurinë. Ndërsa puna nga shtëpia është bërë normalja e re, organizata të ndryshme dhe punonjësit e tyre janë në radarin e kriminelëve kibernetikë.

Prandaj, organizatat duhet të miratojnë masa të sigurisë kibernetike në mënyrë që të zbusin rreziqet kibernetike dhe të luftojnë kërcënimet kibernetike mbizotëruese.

7 REFERENCAT

[1] CISA Department of Homeland Security National, 'Cyber Awareness System', date of publication: 14.11.2019 [https://us-cert.cisa.gov/ncas/tips/ST04-001], date accessed: 06.10.2020.

[2] Cyber Security Insiders, ‘A Brief History of Cybersecurity’, date of publication: 2020 [https://www.cybersecurity-insiders.com/a-brief-history-of-cybersecurity], date accessed: 05.10.2020.

[3] C. Hadnagy, "Social Engineering: The science of human hacking. Christopher Hadnagy”, 2018.

[4] M. Aiken, “The Cyber Effect”, 2016.

[5] K. Mitnick, “The art of invisibility.The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data”, 2017.

[6] GISuser Beyond the map, ‘How Cyber Security Has Evolved in The Last 5 Years’, date of publication: 10.02.2019 [https://gisuser.com/2019/02/from-state-0-to-2019-how-cyber-security-has-evolved-in-the-last-5-years], date accessed: 05.10.2020.

[7] V. R. Sloms dhe V. J. Niekerk, “From information security to cyber security”.Computers & Security”, 2013.

[8] K. &. H. W. Giles, “Divided by a common language: Cyber definitions in Chinese, Russian and English. In K. Podins, J. Stinissen, & M. Maybaum (Eds.), Proceedings of the 5th international conference on cyber conflict”, CCD COE Publications, 2013.

[9] R. S. Dewar, “National cybersecurity and cyberdefense policy snapshots”, Zurich: Center for Security Studies. CSS, ETH Zurich, 2018.

[10] M. &. E. F. J. Dunn Cavelty, “The politics of cybersecurity: Balancing different roles of the state. St Antony’s International Review”, 2019, pp. pp15, 37–57..

[11] D. S. A. D. S. &. T. A. Papp, “Historical impacts of information technologies: An overview”, Washington, DC: National Defense University, 1997, p. pp. 13–35.

[12] K. Schwab, “Shaping the future of the fourth industrial revolution: A guide to building a better world”. New York, NY: Currency, New York, NY: Currency, 2018.

[13] M. D. C. &. A. Wenger, “Cyber security meets security politics: Complex technology, fragmented politics, and networked science, Contemporary Security Policy”, 2020.

[14] J. H. H. &. N. A. W. Hagmann, “The politicisation of security: Controversy, mobilisation. Arena Shifting. European Review of International Studies”, 2019, pp. pp 5, 3,29.

[15] Fast Company, ‘No, remote work isn’t a “new” perk—it’s been around for about 1.4 million years’, date of publication: 16.04.2019 [https://www.fastcompany.com/90330393/the-surprising-history-of-working-from-home], date accessed: 10.10.2020.

[16] We Work Remotely, ‘The History, Evolution and Future of Remote Work’, date of publication: 2020 [https://weworkremotely.com/history-of-remote-work], date accessed: 10.10.2020.

[17] World Health Organization, ‘Coronavirus’, date of publication: 20.03.2020 [https://www:who:int/health-topics/coronavirus], date accessed: 11.10.2020.

[18] W. Markotter, ‘COVID-19: Why it matters that scientists continue their search for source of patient zero's infection', date of publication: 19.03.2020 [https://www:up:ac:za/news/post 2880755-covid-19-why-it-matters- that scientists-continue-their-search-for-source-of-patient-zeros- infection-], date accessed: 11.10.2020.

[19] World Health Organization, ‘WHO Director-General's opening remarks at the media briefing on COVID-19’, date of publication: 20.03.2020 [https://www:who:int/dg/speeches/detail/who-director-general-s-opening-remarks-at-themedia-briefing-on-covid-19---11-march-2020], date accessed: 11.10.2020.

[20] BBC News, ‘Coronavirus: Fake News purveyor to help fight misinformation’, date of publication: 20.03.2020 [https://www:bbc:com/news/uk-england-essex-51929424], date accessed: 11.10.2020.

[21] D. Nelson, ‘Thieves Swindle $2M From Coronavirus Preppers With Hand Sanitizer, Face Mask Scams’, date of publication: 20.03.2020 [https://www:coindesk:com/thieves-swindle-2m-from-coronavirus-preppers-with-hand-sanitizer-face-mask-scams], date accessed: 11.10.2020.

[22] C. Hadnagy, “Social Engineering The Science of Human Hacking”, 2018.

[23] S. Smit, ‘This is what Bill Gates had to say about epidemics, back in 2015’, date of publication: 20.03.2020 [https://www:weforum:org/agenda/2020/03/bill-gates-epidemic-pandemic-preparedness-ebola-covid-19], date accessed: 12.10.2020.

[24] BBC News, ‘Coronavirus: Italy sees rapid spread of fake news’, date of publication: 20.03.2020 [https://www:bbc:com/news/world-europe-51819624], date accessed: 12.03.2020.

[25] BBC News, ‘Coronavirus: The fake health advice you should ignore’, date of publication: 20.03.2020 [https://www:bbc:com/news/world-51735367], date accessed: 12.10.2020.

[26] Department of International Development, ‘UK aid to tackle global spread of coronavirus fake news’, date of publication: 20.03.2020 [https://www:gov:uk/government/news/uk-aid-to-tackle global-spread-of-coronavirus-fake-news], date accessed: 12.10.2020.

[27] Trend Micro, ‘Developing Story: Coronavirus Used in Malicious Campaigns’, date of publication: 11.11.2020 [https://www:trendmicro:com/vinfo/us/security/news/cybercrime-and-digitalthreats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains], date accessed: 11.11.2020.

[28] H. F. A. C. Duncan, ‘Hackers made their own coronavirus map to spread malware, feds warn’, date of publication: 2020 [https://www:miamiherald:com/news/nation-world/national/article241171546:html], date accessed: 12.11.2020.

[29] Federal Trade Commision (FTC), ‘FTC: Coronavirus scams, Part 2’, date of publication: 19.03.2020 [https://www:consumer:ftc:gov/blog/2020/03/ftc-coronavirus-scams-part-2], date accessed: 12.10.2020.

[30] MalwareBytes, ‘Cybercriminals impersonate World Health Organization to distribute fake coronavirus e-book’, date of publication: 15.06.2020 [https://blog.malwarebytes.com/socialengineering/2020/03/cybercriminals-impersonate-worldhealth-organization-to-distribute-fake-coronavirus-ebook/], date accessed: 12.10.2020.

[31] The Times, ‘Fraudsters impersonate airlines and Tesco in coronavirus scams’, date of publication: 15.06.2020 [https://www.thetimes.co.uk/article/fraudstersimpersonate-airlines-and-tesco-in-coronavirus-scams- 5wdwhxq7p], date accessed: 12.10.2020.

[32] Krebs on Security, ‘Live Coronavirus Map Used to Spread Malware’, date of publication: 15.06.2020 [https://krebsonsecurity.com/2020/03/live-coronavirusmap-used-to-spread-malware], date accessed: 13.10.2020.

[33] R. Smithers, ‘Fraudsters use bogus nhs contact-tracing app in phishing scam’, date of publication: 30.05.2020 [https://www.theguardian.com/world/2020/may/13/fraudsters-use-bogus-nhs-contact-tracing-appinphishing-scam], date accessed: 13.10.2020.

[34] Europol, ‘Pandemic Profiteering: How Criminals Exploit COVID-19 Crisis’, date of publication: 15.03.2020 [https://www.europol.europa.eu/publicationsdocuments/ pandemic-profiteering-how-criminalsexploit-covid-19-crisis], date accessed: 13.10.2020.

[35] Norton, ‘Coronavirus Phishing Emails: How to Protect Against COVID-19 Scams’, date of publication: 17.06.2020 [https://us.norton.com/internetsecurity-online-scamscoronavirus-phishing-scams.html], date accessed: 14.10.2020.

[36] The Guardian, ‘US Authorities Battle Surge in Coronavirus Scams, From Phishing to Fake Treatments’, date of publication: 17.06.2020 [https://www.theguardian.com/world/2020/mar/19/coronavirus-scams-phishing-fake treatments], date accessed: 14.10.2020.

[37] J. R. C. Nurse, “Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit, in The Oxford Handbook of Cyberpsychology”, OUP, 2019.

[38] Wired, ‘Hackers Are Targeting Hospitals Crippled by Coronavirus’, date of publication: 15.06.2020 [https://www.wired.co.uk/article/coronavirus-hackerscybercrime-phishing], date accessed: 15.10.2020.

[39] UK’s National Cyber Security Centre (NCSC) and the US’ Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), ‘Advisory: COVID-19 Exploited by Malicious Cyber Actors’ date of publication: 2020 [https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory], date accessed: 15.10.2020.

[40] Mimecast, ‘New Threat Intelligence Report:100 Days of Coronavirus’, date of publication: 19.07.2020 [https://www.mimecast.com/blog/2020/05/100-daysof-coronavirus/], date accessed: 15.10.2020.

[41] NCSC, ‘NCSC Shines Light on Scams Being Foiled via Pioneering New Reporting Service’, date of publication: 17.07.2020 [https://www.actionfraud.police.uk/news/cyber-expertsshine-light-on-online-scams-as-british public-flag-over-160000-suspect-emails], date accessed: 15.10.2020.

[42] Sky News, ‘Coronavirus: Fraud victims have lost more than £4.6m to virus-related scams’, date of publication: 20.07.2020 [https://news.sky.com/story/coronavirus-fraud-victimshave-lost-more-than-4-6m-to-virus-related-scams-11996721], date accessed: 15.10.2020.

[43] J. Tidy, ‘Coronavirus: Israel enables emergency spy powers’, date of publication: 22.07.2020 [https://www.bbc.co.uk/news/technology-51930681], date accessed: 20.10.2020.

[44] M. Hill, ‘HMRC Shuts Down Almost 300 COVID19 Phishing Scam Sites’, date of publication: 02.08.2020 [https://www.infosecuritymagazine.com/news/hmrc-covid19-phishing-scams/], date accessed: 20.10.2020.

[45] U. Government, ‘Budget 2020: What You Need to Know’, date of publication: 2020 [https://www.gov.uk/government/news/budget-2020-what-you-need-to-know], date accessed: 20.10.2020.

[46] Swansea Council, ‘Coronavirus Scams’, date of publication: 10.08.2020 [https://www.swansea.gov.uk/coronavirusscam], date accessed: 10.06.2020.

[47] S. H. R. J. a. L. S. B. Collier, “The implications of the COVID-19 pandemic for cybercrime policing in Scotland: a rapid review of the evidence and future considerations, ser. Research Evidence in Policing: Pandemics. Scottish Institute for Policing Research”, 2020.

[48] Security Boulevard, ‘5 Biggest Cyber Attacks of 2020’, date of publication: 30.10.2020 [https://securityboulevard.com/2020/10/5-biggest-cyber-attacks-of-2020-so-far/], date accessed: 11.11.2020.

[49] Security Boulevard, ‘Biggest Twitter Breach Accounts of US High Profiles Hacked', date of publication: 30.10.2020 [https://securityboulevard.com/2020/07/biggest-twitter-breach-accounts-of-us-high-profiles-hacked-in-bitcoin-scam/], date accessed: 11.11.2020.

[50] Wired.com, ‘How Twitter Survived Its Biggest Hack and Plans to Stop the Next One’, date of publication: 24.09.2020 [https://www.wired.com/story/inside-twitter-hack-election-plan/], date accessed: 11.11.2020.

[51] The National Law Review, ‘Cybersecurity Lessons from the Twitter Hack as New York’s Chief Financial Services Regulator Calls for a Dedicated Cybersecurity Regulator of Large Social Media Companies’, date of publication: 11.02.2020 [https://www.natlawreview.com/article/cybersecurity-lessons-twitter-hack-new-york-s-chief-financial-services-regulator], date accessed: 11.11.2020.